



# **TS-439 Pro Turbo NAS**

## **User Manual (Version: 2.1.0)**



©Copyright 2008. QNAP Systems, Inc. All Rights Reserved.

## FOREWORD

Thank you for choosing QNAP products! This user manual provides detailed instructions of using TS-439 Pro. Please read carefully and start to enjoy the powerful functions of TS-439 Pro!

## NOTE

- "TS-439 Pro" is hereafter referred to as "NAS".
- This manual provides the description of all functions of TS-439 Pro. The product you purchased may not support certain functions dedicated to specific models.
- All features, functionality, and other product specifications are subject to change without prior notice or obligation.
- All brands and products names referred to are trademarks of their respective holders.

## LIMITED WARRANTY

In no event shall the liability of QNAP Systems, Inc. (QNAP) exceed the price paid for the product from direct, indirect, special, incidental, or consequential software, or its documentation. QNAP makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. QNAP reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.



### CAUTION

1. Back up your system periodically to avoid any potential data loss. QNAP disclaims any responsibility of all sorts of data loss or recovery.
2. Should you return any components of the NAS package for refund or maintenance, make sure they are carefully packed for shipping. Any form of damages due to improper packaging will not be compensated.

# Table of Contents

<b>TABLE OF CONTENTS.....</b>	<b>3</b>
<b>SAFETY WARNINGS.....</b>	<b>7</b>
<b>CHAPTER 1. OVERVIEW.....</b>	<b>8</b>
1.1 INTRODUCTION.....	8
1.2 PACKAGE CONTENTS .....	10
1.3 HARDWARE ILLUSTRATION.....	11
<b>CHAPTER 2. INSTALL NAS .....</b>	<b>12</b>
2.1 INSTALL HARD DISK.....	12
2.2 HARD DISK COMPATIBILITY LIST .....	14
2.3 CHECK SYSTEM STATUS .....	17
2.4 CONFIGURE SOFTWARE SETTINGS .....	20
2.4.1 <i>Windows® Users</i> .....	20
2.4.2 <i>Mac Users</i> .....	25
<b>CHAPTER 3. USE THE POWERFUL SERVICES OF THE NAS .....</b>	<b>28</b>
3.1 SERVER ADMINISTRATION .....	34
3.2 QUICK CONFIGURATION .....	35
3.3 SYSTEM SETTINGS.....	41
3.3.1 <i>Server Name</i> .....	41
3.3.2 <i>Date &amp; Time</i> .....	42
3.3.3 <i>Filename Encoding Setting</i> .....	43
3.3.4 <i>Configure SMTP Server</i> .....	43
3.3.5 <i>Configure SMSC Server</i> .....	44
3.3.6 <i>View System Settings</i> .....	45
3.4 NETWORK SETTINGS .....	46
3.4.1 <i>TCP/ IP Configuration</i> .....	46
3.4.2 <i>Microsoft Networking</i> .....	52
3.4.3 <i>Apple Networking</i> .....	54
3.4.4 <i>NFS Service</i> .....	54
3.4.5 <i>Web File Manager</i> .....	54
3.4.6 <i>FTP Service</i> .....	55
3.4.7 <i>Multimedia Station</i> .....	57

3.4.8	<i>iTunes Service</i> .....	57
3.4.9	<i>Download Station</i> .....	58
3.4.10	<i>Web Server</i> .....	59
3.4.11	<i>DDNS Service</i> .....	61
3.4.12	<i>MySQL Server</i> .....	62
3.4.13	<i>Surveillance Station</i> .....	65
3.4.14	<i>System Port Management</i> .....	73
3.4.15	<i>View Network Settings</i> .....	74
3.5	DEVICE CONFIGURATION .....	76
3.5.1	<i>SATA Disk</i> .....	77
3.5.2	<i>RAID Management Tool</i> .....	80
3.5.3	<i>Disk Volume Encryption Management</i> .....	82
3.5.4	<i>iSCSI Target</i> .....	84
3.5.5	<i>External Storage Device</i> .....	85
3.5.6	<i>USB Printer</i> .....	86
3.5.6.1	Windows Users .....	86
3.5.6.2	Mac Users .....	89
3.6	USER MANAGEMENT .....	93
3.6.1	<i>Users</i> .....	93
3.6.1.1	Create user .....	95
3.6.1.2	Create Multiple Users .....	96
3.6.2	<i>User Groups</i> .....	98
3.6.3	<i>Quota</i> .....	105
3.7	NETWORK SHARE MANAGEMENT .....	107
3.7.1	<i>Network Share Management</i> .....	107
3.7.1.1	Create .....	107
3.7.1.2	Property .....	109
3.7.1.3	Access Control .....	110
3.7.1.4	Delete .....	111
3.7.1.5	Restore .....	112
3.7.1.6	NFS Access Control .....	113
3.7.2	<i>Network Share Status</i> .....	114
3.8	SYSTEM TOOLS .....	115
3.8.1	<i>Alert Notification</i> .....	116
3.8.2	<i>Auto Power on/ off Management</i> .....	117
3.8.3	<i>Hardware Settings</i> .....	121
3.8.4	<i>UPS</i> .....	122
3.8.5	<i>Hard Disk S.M.A.R.T.</i> .....	123

3.8.6	<i>System Update .....</i>	<i>124</i>
3.8.7	<i>USB One Touch Copy Backup.....</i>	<i>125</i>
3.8.8	<i>Change Logo.....</i>	<i>126</i>
3.8.9	<i>Back up to an External Storage Device .....</i>	<i>127</i>
3.8.10	<i>Remote Replication (Disaster Recovery) .....</i>	<i>129</i>
3.8.11	<i>Back up/ Restore/ Reset Settings.....</i>	<i>132</i>
3.8.12	<i>IP Filter .....</i>	<i>133</i>
3.8.13	<i>Network Recycle Bin.....</i>	<i>135</i>
3.8.14	<i>Remote Login.....</i>	<i>136</i>
3.8.15	<i>QPKG .....</i>	<i>137</i>
3.8.16	<i>Import SSL Secure Certificate.....</i>	<i>139</i>
3.9	<b>EVENT LOGS.....</b>	<b>140</b>
3.9.1	<i>System Event Logs .....</i>	<i>140</i>
3.9.2	<i>System Connection Logs .....</i>	<i>141</i>
3.9.3	<i>On-line Users.....</i>	<i>143</i>
3.9.4	<i>System Information .....</i>	<i>143</i>
3.9.5	<i>Syslog Settings .....</i>	<i>144</i>
<b>CHAPTER 4.</b>	<b>USE FRONT USB BACKUP BUTTON.....</b>	<b>145</b>
<b>CHAPTER 5.</b>	<b>MULTIMEDIA STATION .....</b>	<b>146</b>
5.1	<i>SHARE PHOTOS AND MULTIMEDIA FILES VIA WEB INTERFACE .....</i>	<i>146</i>
5.2	<i>ENABLE ITUNES SERVICE .....</i>	<i>156</i>
5.3	<i>USE UPNP MEDIA SERVER .....</i>	<i>159</i>
<b>CHAPTER 6.</b>	<b>DOWNLOAD STATION.....</b>	<b>162</b>
6.1	<i>USE DOWNLOAD SOFTWARE QGET .....</i>	<i>172</i>
<b>CHAPTER 7.</b>	<b>WEB SERVER.....</b>	<b>174</b>
<b>CHAPTER 8.</b>	<b>FTP SERVER.....</b>	<b>178</b>
<b>CHAPTER 9.</b>	<b>WEB FILE MANAGER.....</b>	<b>181</b>
<b>CHAPTER 10.</b>	<b>NETBAK REPLICATOR .....</b>	<b>186</b>
<b>CHAPTER 11.</b>	<b>CONFIGURING AD AUTHENTICATION .....</b>	<b>201</b>
<b>CHAPTER 12.</b>	<b>ACCESS THE NAS FROM LINUX .....</b>	<b>206</b>
<b>CHAPTER 13.</b>	<b>NAS MAINTENANCE.....</b>	<b>207</b>
13.1	<i>RESTART/ SHUT DOWN SERVER .....</i>	<i>207</i>
13.2	<i>RESET ADMINISTRATOR PASSWORD AND NETWORK SETTINGS.....</i>	<i>208</i>
13.3	<i>DISK FAILURE OR MALFUNCTION .....</i>	<i>209</i>

13.4	POWER OUTAGE OR ABNORMAL SHUTDOWN.....	209
13.5	ABNORMAL OPERATION OF SYSTEM SOFTWARE.....	209
13.6	SYSTEM TEMPERATURE PROTECTION .....	209
<b>CHAPTER 14.</b>	<b>RAID ABNORMAL OPERATION TROUBLESHOOTING .....</b>	<b>210</b>
<b>APPENDIX A</b>	<b>USE THE LCD PANEL.....</b>	<b>212</b>
<b>TECHNICAL SUPPORT.....</b>		<b>218</b>
<b>GNU GENERAL PUBLIC LICENSE .....</b>		<b>219</b>

## **Safety Warnings**

1. The NAS can operate normally in the temperature of 0°C-40°C and relative humidity of 0%-95%. Please make sure the environment is well-ventilated.
2. The power cord and devices connected to the NAS must provide correct supply voltage (100W, 90-264V).
3. Do not place the NAS in direct sunlight or near chemicals. Make sure the temperature and humidity of the environment are in optimized level.
4. Unplug the power cord and all connected cables before cleaning. Wipe the NAS with a dry towel. Do not use chemical or aerosol to clean the NAS.
5. Do not place any objects on the NAS for the server's normal operation and to avoid overheat.
6. Use the flat head screws in the product package to lock the hard disks in the NAS when installing hard disks for proper operation.
7. Do not place the NAS near any liquid.
8. Do not place the NAS on any uneven surface to avoid falling off and damage.
9. Make sure the voltage is correct in your location when using the NAS. If you are not sure, please contact the distributor or the local power supply company.
10. Do not place any object on the power cord.
11. Do not attempt to repair your NAS in any occasions. Improper disassembly of the product may expose you to electric shock or other risks. For any enquiries, please contact the distributor.

# Chapter 1. Overview

## 1.1 Introduction

Thank you for choosing QNAP NAS. Your NAS supports the following key features:

### **File Server**

- File sharing across Windows/ Mac/Linux/ Unix and centralized management

### **FTP Server**

- Support data access from remote location via FTP (max. 256 simultaneous connections)
- FTP with SSL/ TLS (explicit) mode
- FXP supported
- FTP bandwidth control and connection control
- Passive FTP port range control

### **Backup Server**

- QNAP client-side backup software -NetBak Replicator  
Supports instant, schedule, and auto-sync backup
- 3rd party backup software support:  
Acronis True Image, CA Brightstor, ARCserve Backup, EMC Retrospect, Symantec Backup Exec, LaCie Silverkeeper

### **RAID Station**

- Advanced disk configurations: RAID 0, 1, 5, 6, 5 + spare, single and JBOD.
- Intelligent on-line RAID capacity expansion and RAID level migration

### **Printer Server**

- Network printer sharing via USB (support Windows & Mac platform)
- Support all-in-one printer (max. 3 sets)

### **Remote Replication**

- Data on the NAS can be backed up to or from another Turbo NAS or Rysnc server over the network securely.

### **Web Server**

- Built-in phpMyAdmin, built-in Joomla!, editable php.ini, SQLite and MySQL

### **MySQL Server**

- Support MySQL database server

### **UPnP MediaServer (built-in TwonkyMedia)**

- Support UPnP/ DLNA multimedia technology; share stored photos and home videos on TV, listen to music on Hi-Fi system via DMP



- Enjoy more than hundreds of worldwide Internet radio (built-in
- TwonkyMedia)
- Support media playing with PS3, Xbox360, PSP game consoles

#### **iTunes Server**

- iTunes server for music sharing on your network
- Support Smart Playlist for iTunes software

#### **Multimedia Station**

- Image slide show and rotation (+90°, -90°)
- Display photo details: dates, exposure time, aperture, etc
- Automatic thumbnail generation for easy browsing
- Photo album access authority management
- Multimedia files (video and audio) local playing
- Automatic file categorization

#### **Download Station**

- Support PC-less BitTorrent/ FTP/ HTTP download
- QNAP remote download control software: QGet (Windows/ Mac), allows you to control the download tasks of multiple Turbo NAS on one PC via LAN/ WAN
- BitTorrent download supports TCP/UDP, DHT
- BT schedule download supported
- Support BT tasks download (up to 500)
- Download configuration (current seed number, configurable port range, bandwidth control, download percentage, UPnP NAT port forwarding for BitTorrent download)
- Download status list management (download percentage)
- Support access from Mac by Mozilla Firefox

## 1.2 Package Contents

Your NAS package contains:

- ✓ TS-439 Pro Turbo NAS



- ✓ Power cord



- ✓ CD-ROM (user manual, QNAP Finder & utility inclusive)



- ✓ Quick Installation Guide



- ✓ Flat head screw x 16



- ✓ Ethernet cable x 2



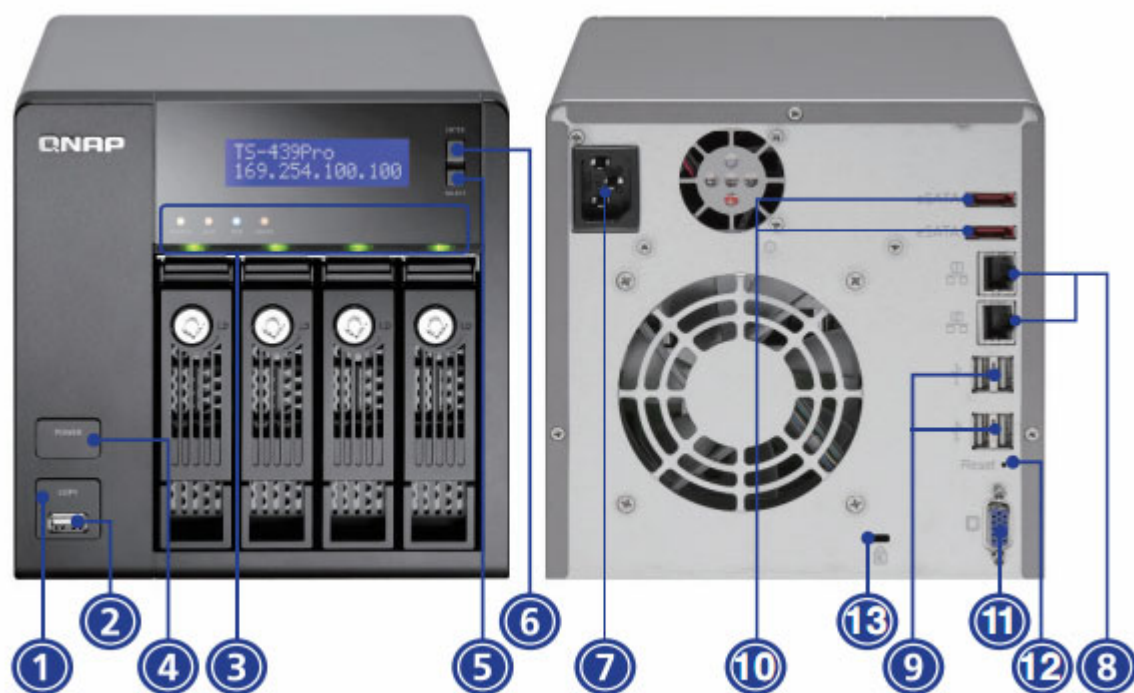
- ✓ Hard disk lock



- ✓ Quick Installation Guide (RAID configuration)



## 1.3 Hardware Illustration



1. One touch copy button
2. USB 2.0
3. LED indicators: Status, LAN, USB, eSATA, HDD1, HDD2, HDD3, HDD4
4. Power button
5. Select button
6. Enter button
7. Power connector
8. Giga LAN x 2
9. USB 2.0 x 4
10. eSATA x 2
11. VGA (Reserved)
12. Password & network settings reset button
13. K-lock security slot

## Chapter 2. Install NAS

### 2.1 Install Hard Disk

1. Take out the disk trays.



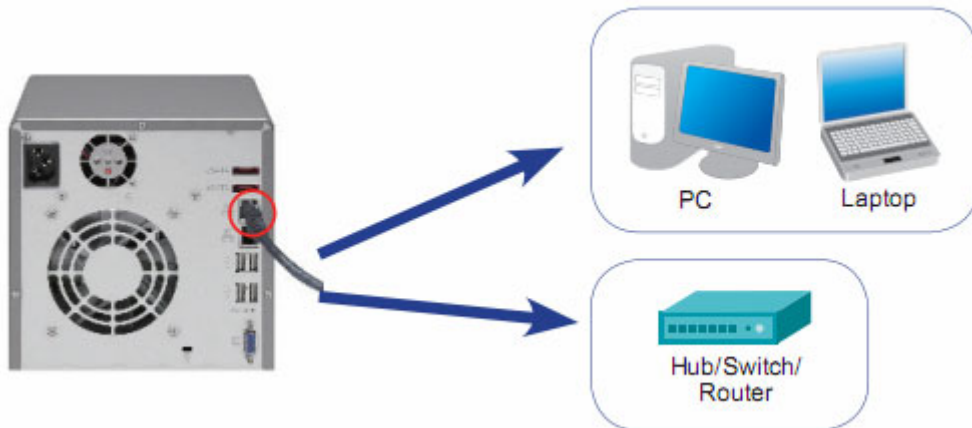
2. Install a hard disk on each tray. Make sure the disk holes match the holes at the base of the disk tray and lock the disk with four screws.



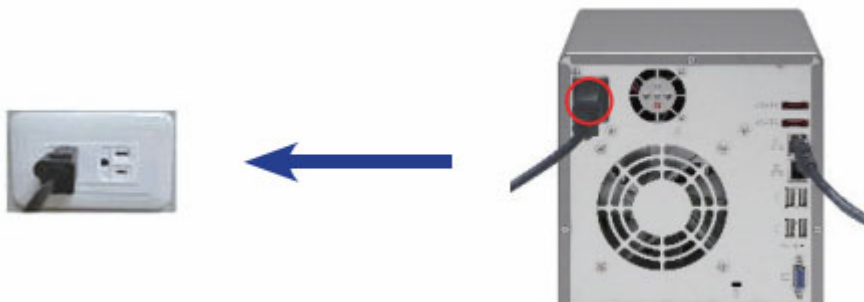
3. Insert the disk trays to NAS. Push the disk trays to the end.



4. Connect the network cable.



5. Connect the power cord to the NAS and plug in the power cord to the wall socket.



## 2.2 Hard Disk Compatibility List

The following HDD models are verified by QNAP that are compatible with the NAS. It is recommended to use the disk models listed here. Other HDD brands that are not tested by QNAP may or may not work properly with the NAS. For more updated compatible hard disk information, please visit QNAP website at <http://www.qnap.com>.



**QNAP disclaims any responsibility for product damage/ malfunction or data loss/ recovery due to misuse or improper installation of hard disks in any occasions for any reasons.**

Brand	Product Family	Model	Interface	RPM	Drive size (GB)	Buffer Size (MB)
Hitachi	Deskstar 7K1000	HDS721010KLA330	SATA II	7200	1000	32
Hitachi	Deskstar 7K1000	HDS721075KLA330	SATA II	7200	750	32
Hitachi	Deskstar E7K500	HDS725050KLA360	SATA II	7200	500	16
Hitachi	Deskstar T7K500	HDT725025VLA380	SATA II	7200	500	8
Hitachi	Deskstar T7K500	HDT725040VLA360	SATA II	7200	400	16
Hitachi	Deskstar T7K500	HDT725040VLA380	SATA II	7200	400	8
Hitachi	Deskstar T7K500	HDT725032VLA360	SATA II	7200	320	16
Hitachi	Deskstar T7K500	HDT725032VLA380	SATA II	7200	320	8
Hitachi	Deskstar T7K500	HDT725025VLA360	SATA II	7200	250	16
Hitachi	Deskstar T7K500	HDT725025VLA380	SATA II	7200	250	8
Hitachi	Deskstar T7K250	HDT722525DLA380	SATA II	7200	250	8
Hitachi	Deskstar T7K250	HDT722516DLA380	SATA II	7200	160	8
Hitachi	Deskstar P7K500	HDP725050GLA380	SATA II	7200	500	16
Hitachi	Deskstar P7K500	HDP725050GLA360	SATA II	7200	500	8
Hitachi	Deskstar P7K500	HDP725040GLA380	SATA II	7200	400	16
Hitachi	Deskstar P7K500	HDP725040GLA360	SATA II	7200	400	8
Hitachi	Deskstar P7K500	HDP725032GLA380	SATA II	7200	320	16
Hitachi	Deskstar P7K500	HDP725032GLA360	SATA II	7200	320	8

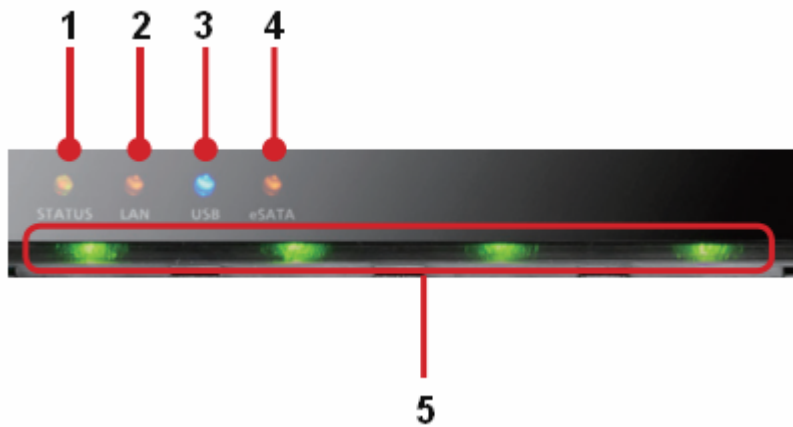
Hitachi	Deskstar P7K500	HDP725025GLA380	SATA II	7200	250	8
Seagate	Barracuda ES	ST3750640NS	SATA II	7200	750	16
Seagate	Barracuda ES	ST3500630NS	SATA II	7200	500	16
Seagate	Barracuda ES	ST3400620NS	SATA II	7200	400	16
Seagate	Barracuda ES	ST3320620NS	SATA II	7200	320	16
Seagate	Barracuda ES	ST3250620NS	SATA II	7200	250	16
Seagate	Barracuda ES	ST3250820NS	SATA II	7200	250	8
Seagate	Barracuda ES.2	ST31000340NS	SATA II	7200	1000	32
Seagate	Barracuda ES.2	ST3750330NS	SATA II	7200	750	32
Seagate	Barracuda ES.2	ST3500320NS	SATA II	7200	500	32
Seagate	Barracuda ES.2	ST3250310NS	SATA II	7200	250	32
Seagate	Barracuda 7200.11	ST31000340AS	SATA II	7200	1000	32
Seagate	Barracuda 7200.11	ST3750330AS	SATA II	7200	750	32
Seagate	Barracuda 7200.11	ST3750630AS	SATA II	7200	750	16
Seagate	Barracuda 7200.11	ST3500320AS	SATA II	7200	500	32
Seagate	Barracuda 7200.11	ST3500620AS	SATA II	7200	500	16
Seagate	Barracuda 7200.11	ST3320613AS	SATA II	7200	320	16
Seagate	Barracuda 7200.10	ST3250620AS	SATA II	7200	250	16
Seagate	Barracuda 7200.10	ST3250410AS	SATA II	7200	250	16
Seagate	Barracuda 7200.10	ST3250310AS	SATA II	7200	250	8
Seagate	Barracuda 7200.10	ST3250820AS	SATA II	7200	250	8
Seagate	Barracuda 7200.10	ST3200820AS	SATA II	7200	200	8
Seagate	Barracuda 7200.10	ST3160815A	SATA II	7200	160	8
Seagate	Barracuda 7200.10	ST3160815AS	SATA II	7200	160	2
Seagate	Barracuda 7200.10	ST3160215A	SATA II	7200	160	8
Seagate	Barracuda 7200.10	ST3160215AS	SATA II	7200	160	2
Seagate	Barracuda 7200.10	ST380815AS	SATA II	7200	80	8
Seagate	Barracuda 7200.10	ST380215AS	SATA II	7200	80	2

WD	WD RE2	WD7500AYYS	SATA II	7200	750	16
WD	WD RE2	WD5001ABYS	SATA II	7200	500	16
WD	WD RE2	WD5000ABYS	SATA II	7200	500	16
WD	WD RE2	WD4001ABYS	SATA II	7200	400	16
WD	WD RE2	WD4000ABYS	SATA II	7200	400	16
WD	WD RE2	WD3201ABYS	SATA II	7200	320	16
WD	WD RE2	WD2502ABYS	SATA II	7200	250	16
WD	WD RE2	WD1601ABYS	SATA II	7200	160	16
WD	WD RE2-GP	WD1000FYPS	SATA II	7200	1000	16
WD	WD RE2-GP	WD7500AYPS	SATA II	7200	750	16
WD	WD RE2-GP	WD5000ABPS	SATA II	7200	500	16
WD	WD Caviar Green	WD10EACS	SATA II	7200	1000	16
WD	WD Caviar Green	WD7500AACS	SATA II	7200	750	16
WD	WD Caviar Green	WD5000AACS	SATA II	7200	500	16
WD	WD Caviar SE16	WD7500AAKS	SATA II	7200	750	16
WD	WD Caviar SE16	WD6400AAKS	SATA II	7200	640	16
WD	WD Caviar SE16	WD5000AAKS	SATA II	7200	500	16
WD	WD Caviar SE16	WD4000AAKS	SATA II	7200	400	16
WD	WD Caviar SE16	WD3200AAKS	SATA II	7200	320	16
WD	WD Caviar SE16	WD2500AAKS	SATA II	7200	250	16
Samsung	Spinpoint F1	SAMSUNG HD103UJ	SATA II	7200	1000	32
Samsung	Spinpoint F1	SAMSUNG HD753LJ	SATA II	7200	750	32



## 2.3 Check System Status

The LED indicators of the NAS indicate the system status and information easily. When the NAS is turned on, please check the following items to make sure the system status is normal. Note that the following LED information is applicable only when you have properly installed HDD, and connected the NAS to the network and power.



1. Status
2. LAN
3. USB
4. eSATA
5. HDD1~HDD4

## LED Display & System Status Overview

LED	Color	LED Response	Description
USB	Blue	Flashes every 0.5 sec	1) A USB device is being detected by any USB port 2) Removing USB device 3) Read/ Write (only for front USB) 4) Backup to external USB disk is in process
		ON	USB device is ready (only for front panel USB)
		OFF	Front panel USB copy complete
eSATA	Orange	Flashes	Accessing data
System Status	Red/ Green	Flashes green/red alternately, every 0.5 sec	1) HDD is formatting/ system is initializing 2) Firmware is being updated 3) RAID rebuilding 4) RAID capacity expansion 5) RAID level migration
		Red ON	1) HDD invalid 2) Volume is full 3) Volume is going to be full 4) Fan out of function 5) HDD read/write error 6) HDD bad sector 7) RAID degraded mode(read only) 8) (Hardware self-test error)
		Flashes red every 0.5 sec	Degraded mode
		Flashes green, every 0.5 sec	1) System booting 2) System is not configured 3) HDD is not formatted
		Green ON	System is ready
		Off	All HDD in standby mode
HDD	Red/ Green	Flashes red	HDD access when disk read/write error
		Red ON	HDD read/write error
		Flashes green	HDD access
		Green ON	HDD power on
LAN	Orange	Orange always ON	LAN connected
		Flashes	LAN Access

**Beep Alarm (beep alarm can be disabled in "System Tools" > "Hardware Settings")**

<b>Beep</b>	<b>No. of Times</b>	<b>Description</b>
Short beep (0.5 sec)	1	1) System is booting 2) System is shut down (by software control) 3) Reset 4) Firmware is completely updated
Short beep (0.5 sec)	3	Front USB copy button cannot copy, when backup to external disk is in process
Short beep (0.5 sec), long beep (1.5 sec)	3, every 5 min	Fan out of function
Long beep (1.5 sec)	2	1) HDD volume is going to be full 2) HDD is full 3) HDD in degraded mode 4) HDD starts rebuilding
	1	1) Hardware shutdown 2) System is ready

## 2.4 Configure Software Settings

After checking the system status, please follow the steps below to configure the software settings of the NAS. The configuration procedure of Windows and Mac users are different. Please select the appropriate procedure according to your OS.

### 2.4.1 Windows® Users

1. Execute the product CD, a menu is shown. Select your NAS model to continue.



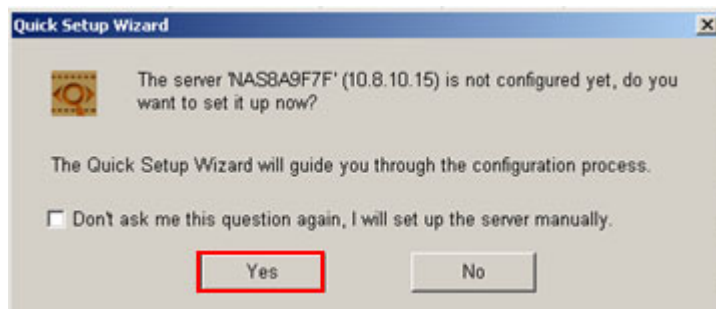
2. The following menu is shown. Select "Install QNAP Finder" to continue.



3. Follow the instructions to install QNAP Finder. QNAP Finder will run automatically. If you are using Windows XP SP2, the following screen will be shown. Please select "Unblock".



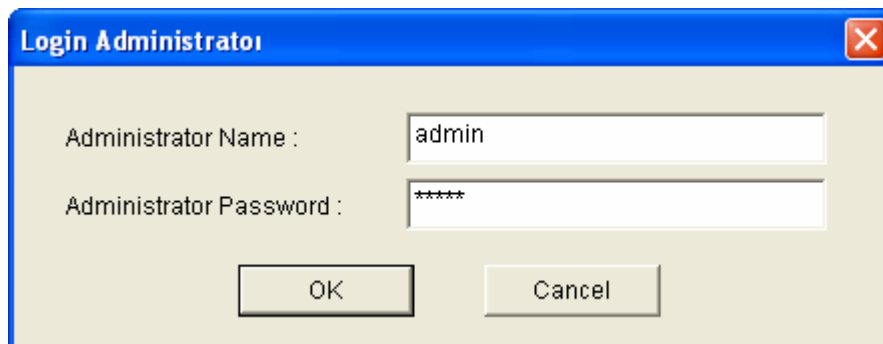
4. QNAP Finder will find the NAS available in the network and ask if you want to perform quick setup. Click "Yes" to continue.



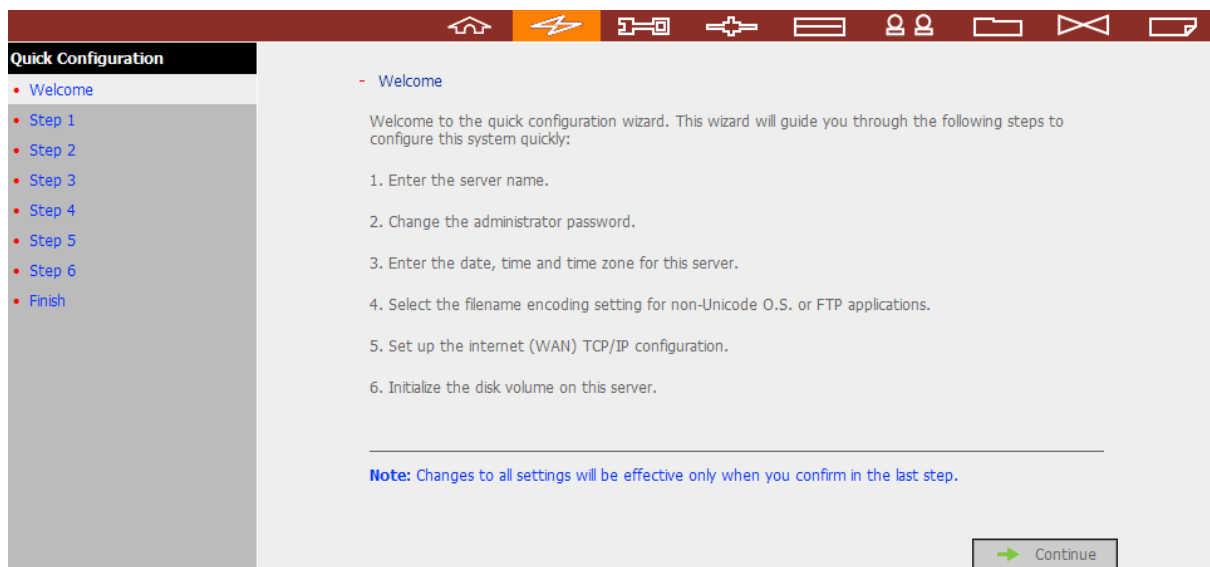
**Note:** If the server is not found, click "Refresh" to try again.

5. Enter the default user name and password.

Default user name: **admin**  
Password: **admin**

A dialog box titled "Login Administrator" with a blue header bar and a close button (X) in the top right corner. The background is a light beige color. It contains two text input fields. The first field is labeled "Administrator Name :" and contains the text "admin". The second field is labeled "Administrator Password :" and contains six asterisks "\*\*\*\*\*". Below the fields are two buttons: "OK" and "Cancel".

6. The quick configuration page will be shown. Click "Continue" and follow the instructions to finish the configuration. For further information, please refer to Chapter 3.2.

A screenshot of a web-based "Quick Configuration" wizard. The interface has a dark red header bar with several navigation icons. On the left, there is a sidebar with a "Quick Configuration" section containing a list of steps: "Welcome", "Step 1", "Step 2", "Step 3", "Step 4", "Step 5", "Step 6", and "Finish". The main content area is light gray and displays the "Welcome" step. It includes a welcome message, a list of six configuration steps, and a "Note" at the bottom stating that changes are only effective after the final step. A "Continue" button with a green arrow is located at the bottom right of the main content area.

**Note:**

1. It is recommended to use Internet Explorer 6.0 or above to access the NAS. If the OS of your PC is Windows® 98, the NAS supports Internet Explorer 6.0 or above only.
2. The NAS also supports Mozilla Firefox.

7. Click "Start installation" to execute the quick configuration.

[Finish](#)

The changes you have made to the server are as below. Click "Start installation" to begin the quick configuration; or click "Back" to return to the previous steps to modify the settings.

Server Name :	NASBA9B4C	
Password:	The password is unchanged.	
Time Zone :	(GMT+08:00) Taipei	
Time Setting:	2008/12/24 16:13:44	
Network :	Obtain TCP/IP settings automatically via DHCP	
Primary DNS Server	0.0.0.0	
Secondary DNS Server	0.0.0.0	
Network services:	Microsoft Networking, Web File Manager, FTP Service, Download Station, Multimedia Station	
Disk configuration:	Do not set disk configuration	
Encrypt disk volume:	No	
Drive 1:	--	--
Drive 2:	Seagate ST31000340AS SD15	931.51 GB
Drive 3:	Seagate ST3160827AS 3.42	149.05 GB
Drive 4:	Seagate ST3500320AS SD15	465.76 GB


[Back](#) [Start installation](#)

8. Congratulations! You have finished the quick configuration. Click "Return to the system administration page" to return to the login page of the NAS.

System is initializing, please wait.

The system is being configured, do NOT power off the server or unplug the hard drive(s).

1. Change the name for this server. ✓
2. Change the administrator password. ✓
3. Change the time settings. ✓
4. Change the network settings. ✓
5. Start the network services. ✓
6. Initialize the hard disk. ✓

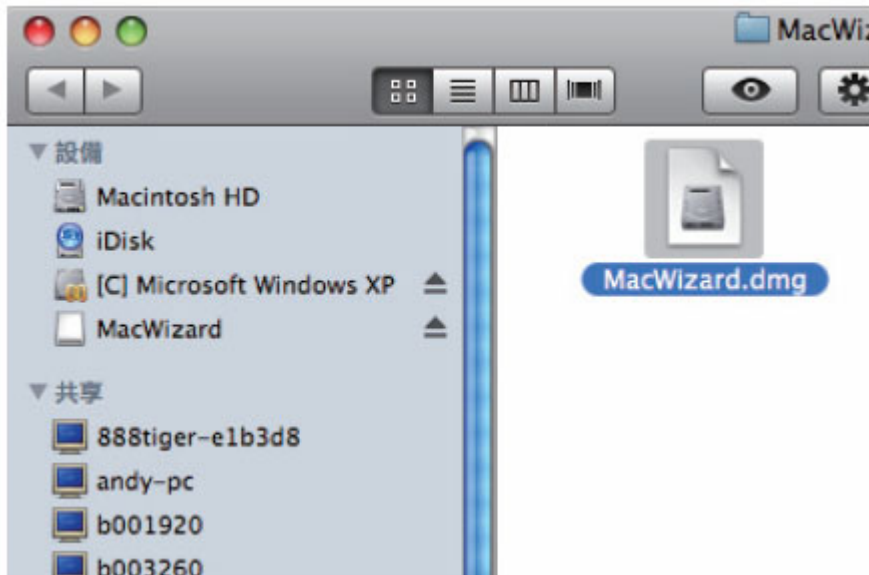
 System configuration completed. [Return to system administration page.](#)

**Note: To use Joomla and phpMyAdmin, please update the system firmware with the image file enclosed in the product CD or install the applications through QPKG.**

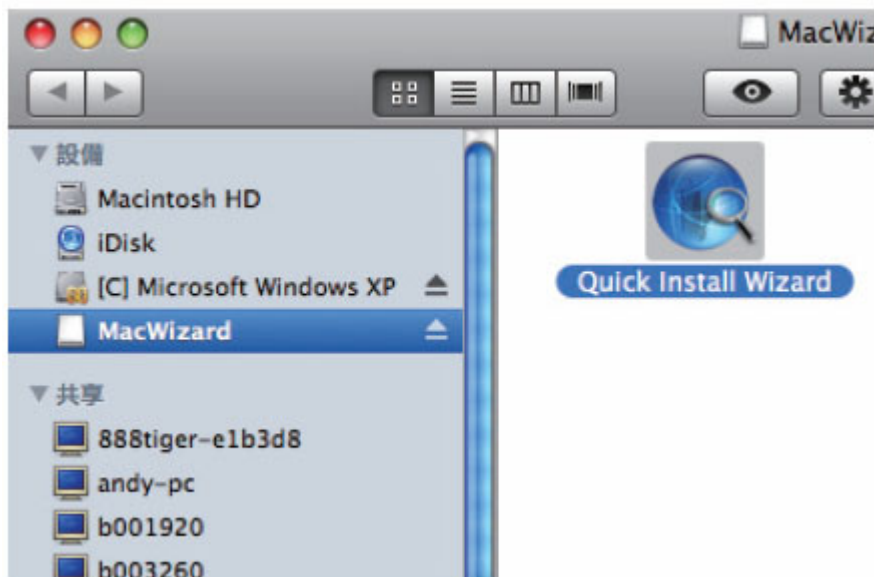


## 2.4.2 Mac Users

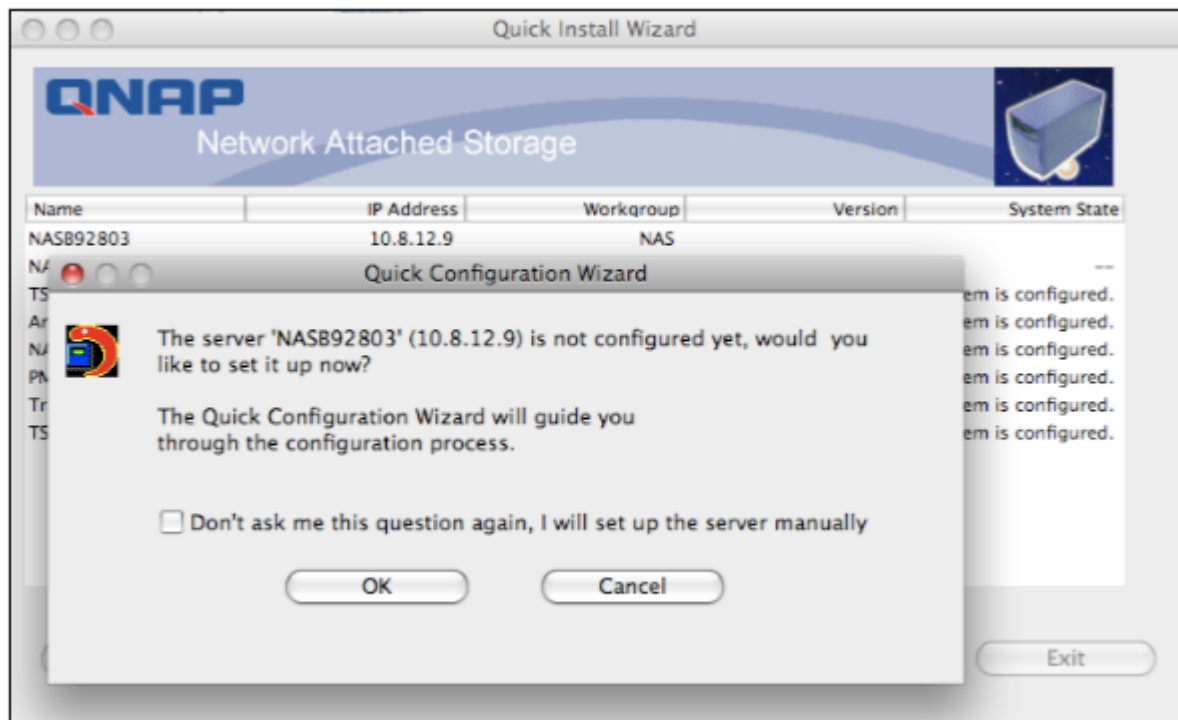
1. Insert the NAS CD-ROM in your Mac and find the directory **Mac Wizard**. Then run **MacWizard.dmg**.



2. Run Quick Install Wizard.

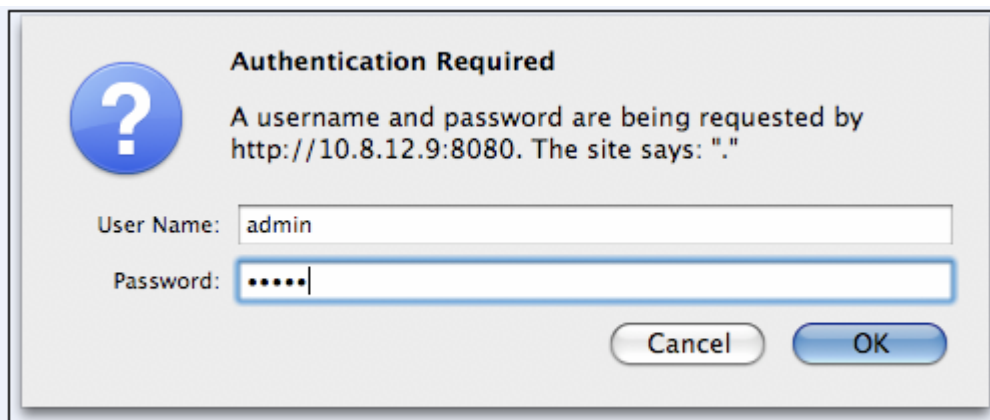


3. The Quick Install Wizard will find the NAS available in the network and ask if you want to perform quick setup. Click "OK" to continue.

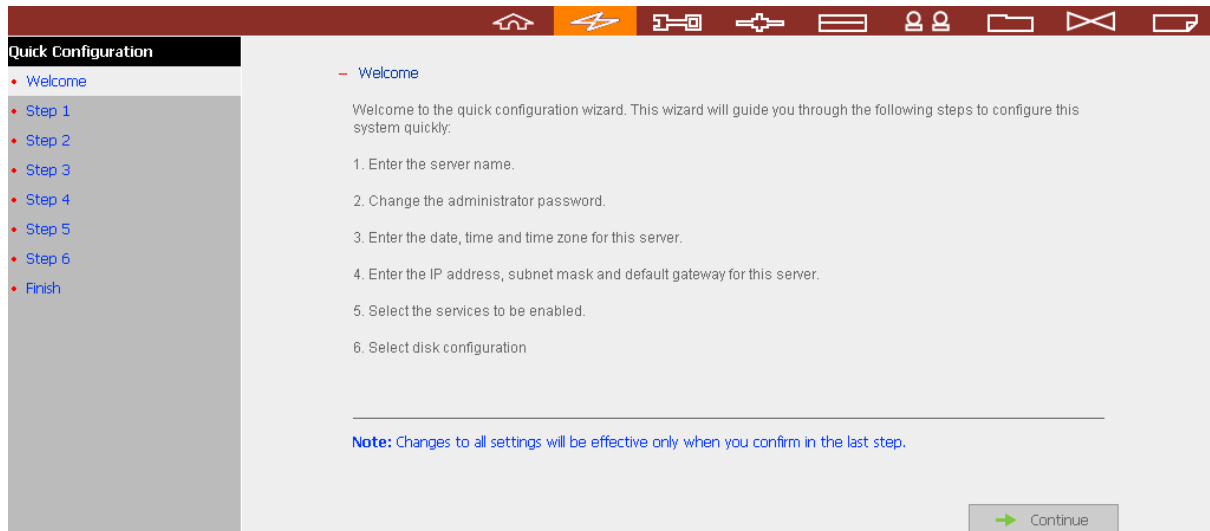


4. Enter the default user name and password.

Default user name: **admin**  
Password: **admin**



5. The quick configuration page will be shown. Click "Continue" and follow the instructions to finish the configuration. For further information, please refer to Chapter 3.2.



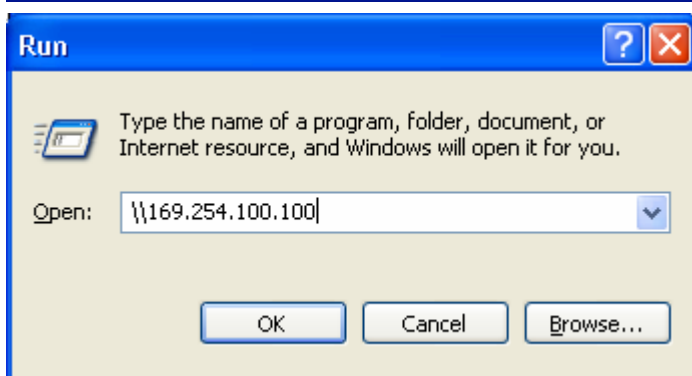
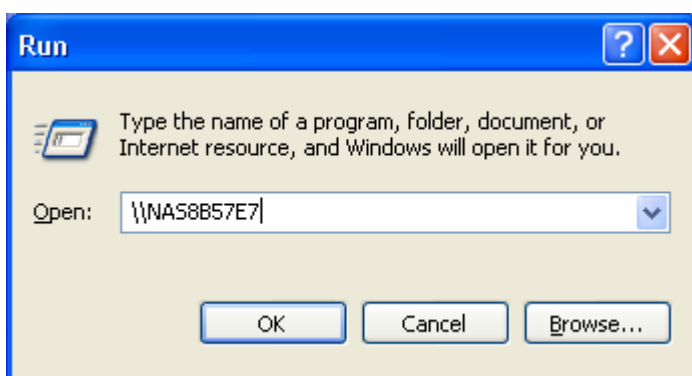
**Note:**

1. Mac Quick Install Wizard does not support mapping network drive.
2. It is recommended to access the NAS by Mozilla Firefox in Mac. Safari does not support Download Station of the NAS.

## Chapter 3. Use the Powerful Services of the NAS

### A. Use network share-Public folder

1. You can access the public folder of the NAS by the following means:
  - a. Open My Network Places and find the workgroup of the NAS. If you cannot find the server, please browse the whole network to search for the NAS. Double click the name of the NAS for connection.
  - b. Use Run function in Windows®. Enter **\\[NAS name]** or **\\[NAS IP]** to access share folder on the NAS.



- c. Windows® users can use the Finder to find the NAS. When the administration page is shown, click "Web File Manager". Enter the user name and password, and then start to manage the NAS.
2. You can upload files to the Public folder.

## **B. Manage the NAS**

### ■ **Manage the NAS using web browser by Windows® or Mac**

1. You can access the NAS web administration page by the following methods:
  - a. Use the Finder to find the NAS.
  - b. Open a web browser and enter **http://[NAS IP]:8080#**



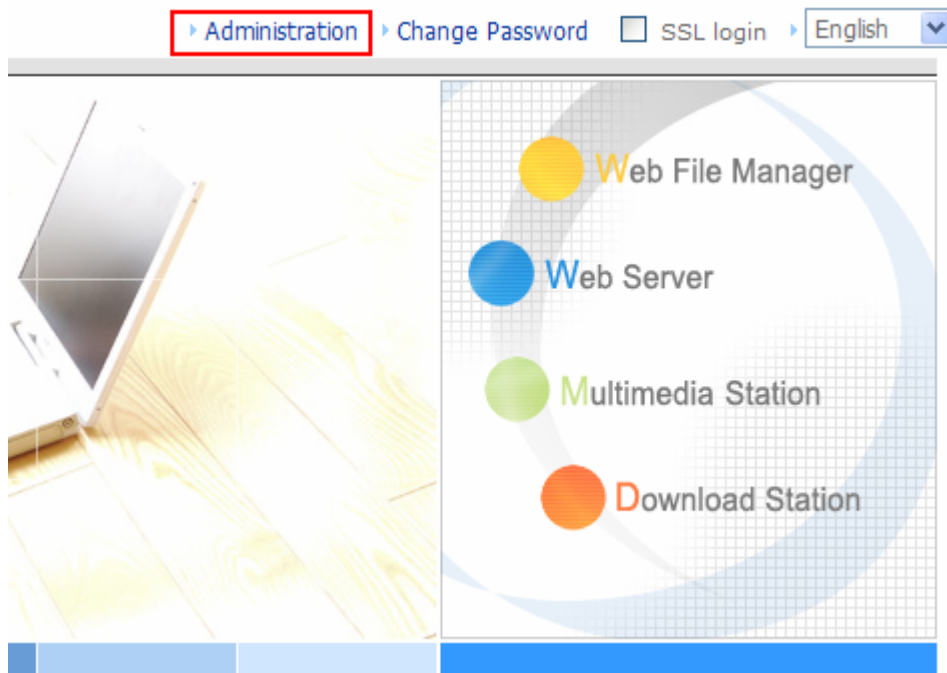
#### **Note:**

1. It is recommended to use Microsoft® Internet Explorer 6.0 or above to access the NAS. If the OS of your PC is Windows® 98, the NAS supports Internet Explorer 6.0 only.
2. Please use Mozilla Firefox to access the NAS in Mac.

**#** If you are using DHCP: (a) connect the PC to the NAS directly, please use the default IP address 169.254.100.100 of the NAS; (b) connect the NAS by network, please run the Finder to view the IP address of the NAS.

2. When the administration page of the NAS is shown, you can start to use the services. To modify system settings, click "Administration". Enter the user name and password to login.

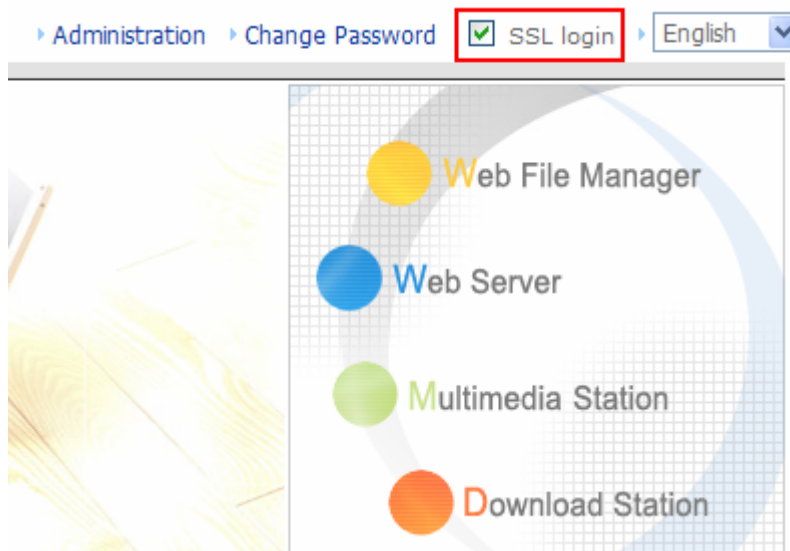
Default user name: **admin**  
Password: **admin**



3. The NAS supports SSL secure login which enables you to configure and manage the server by encrypted transfer. To use this function, check the box **SSL login** on the administration page and login the server.



**Note:** If your NAS is placed behind an NAT gateway and you want to access the NAS by secure login from the Internet, you must open the port 443 on your NAT and forward this port to the LAN IP of the NAS.



## **C. Use the NAS Services**

### **■ Multimedia Station**

The NAS provides a user-friendly web management interface for you to manage and share personal albums and multimedia files via network easily. Supports embedded iTunes Server music sharing, UPnP and DLNA standard multimedia technology to establish home multimedia sharing center. Please refer to Chapter 5.

### **■ Download Station**

The NAS supports BT, FTP, and HTTP download. You can add download tasks to the NAS and let the server finish downloading independently of your PC. Please refer to Chapter 6.

### **■ Advanced RAID Configuration**

The NAS supports single disk volume, linear disk volume, and RAID 0/ 1/ 5/ 6 disk volumes for advanced data protection. Please refer to Chapter 3.5.1.

### **■ Disaster Recovery**

The NAS supports remote share folder backup via the network. In case of data damage in PC, you can restore all backup data. Please refer to Chapter 3.8.10.

### **■ Web Server**

The NAS enables you to create your own website easily. It also supports Joomla! PHP and SQLite to establish interactive websites. Please refer to Chapter 7.

### **■ Printer Server**

The NAS supports network printer sharing function by direct USB connection. No extra help from PC is needed. Please refer to Chapter 3.5.6.

### **■ FTP Server**

The NAS offers the simplest FTP server setup procedure for you to establish FTP server without any professional assistance. Please refer to Chapter 8.

### **■ Backup Server**

NetBak Replicator is the powerful backup software designed for Windows users to configure automatic backup schedule. Block level remote replication is supported to provide the most reliable, instant, and secure data backup mechanism. Please



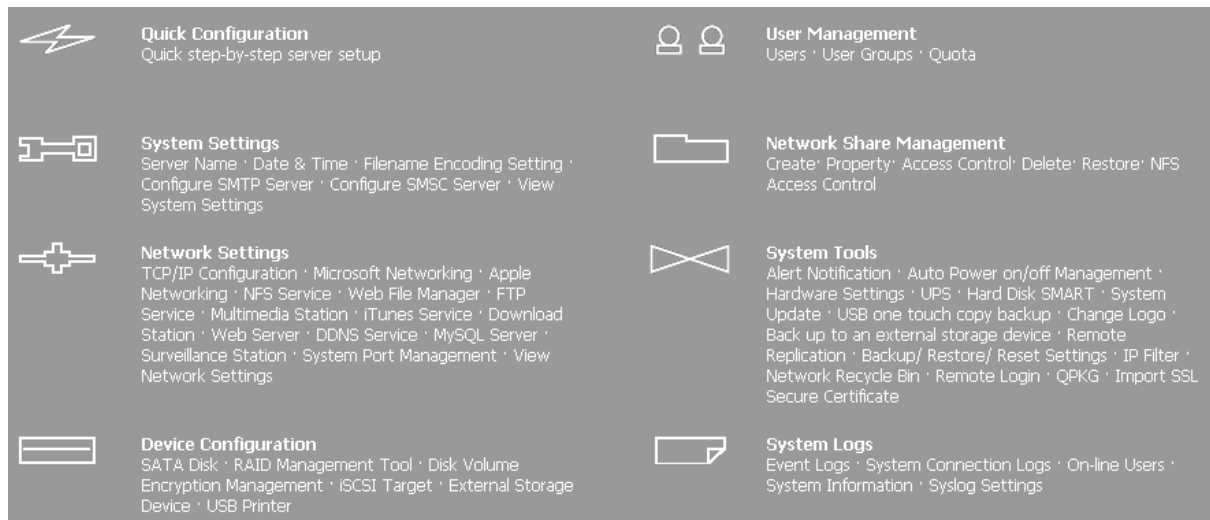
refer to Chapter 10.

#### ■ **File Server**


The NAS provides convenient and secure file server functions that support central data management. Users can be granted with the right to access network share and share important files. Please refer to Chapter 3.7 and Chapter 9.


## 3.1 Server Administration


There are 8 main sections in server administration:




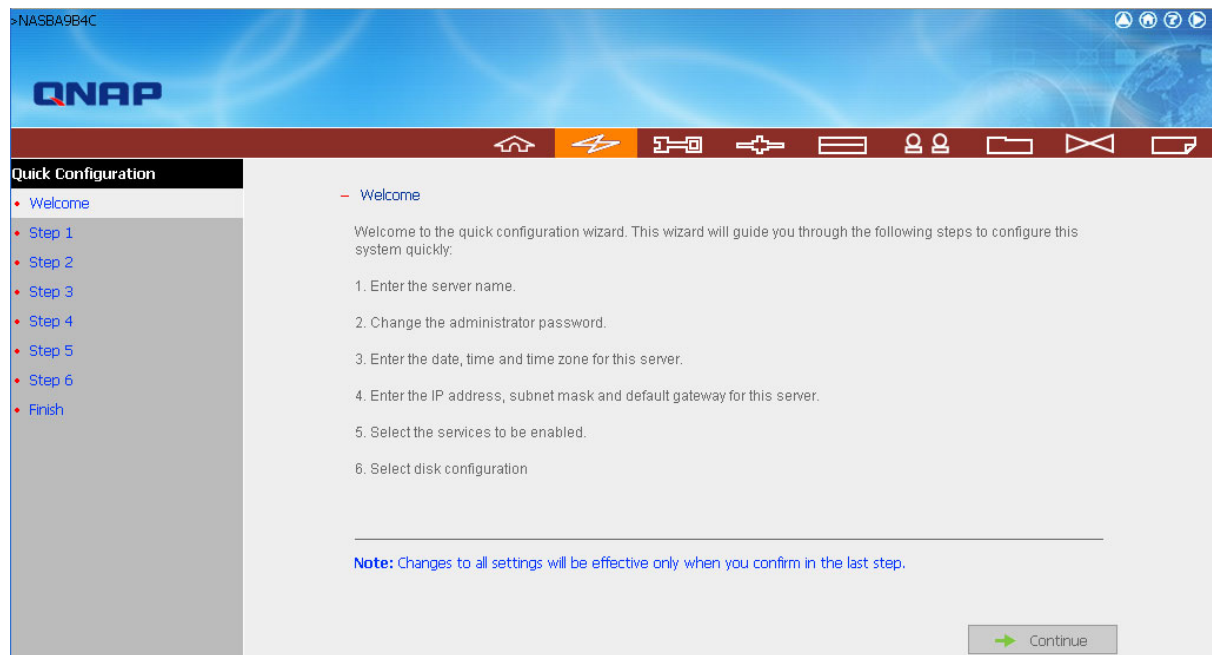
## 3.2 Quick Configuration

Please follow the step-by-step guide in Quick Configuration to complete the settings of the NAS. If you have any questions during web administration, please click the help button  on the top right hand corner of the page. Other buttons are described as below:

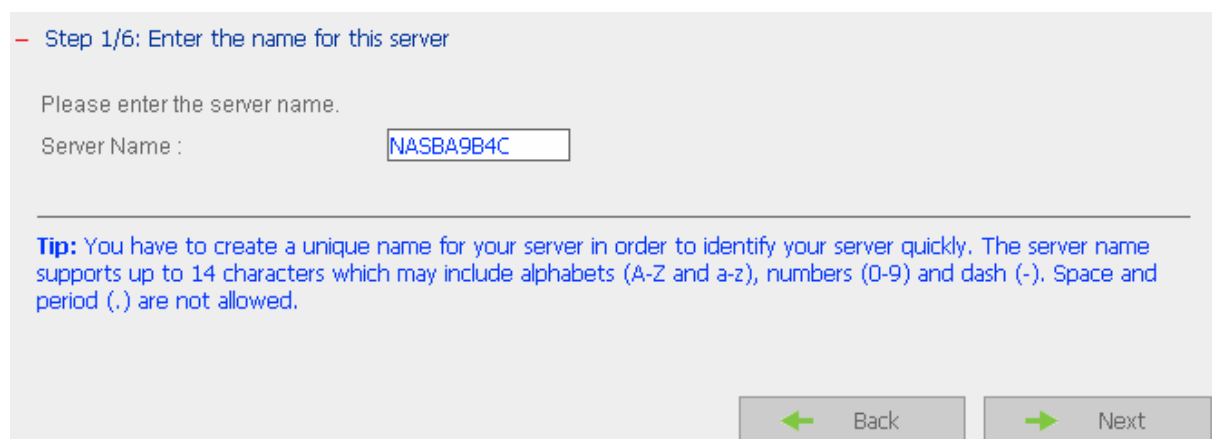
: Return to previous page

: Return to home page

: Logout system



Step 1. Enter the server name.

The screenshot shows the 'Step 1/6: Enter the name for this server' screen. It prompts the user to 'Please enter the server name.' and has a text input field labeled 'Server Name :'. The field contains the text 'NASBA9B4C'. Below the input field, a tip is provided: 'Tip: You have to create a unique name for your server in order to identify your server quickly. The server name supports up to 14 characters which may include alphabets (A-Z and a-z), numbers (0-9) and dash (-). Space and period (.) are not allowed.' At the bottom, there are two buttons: 'Back' and 'Next'.

Step 2. Change the administrator password or select to use the original password.

- Step 2/6: Change the administrator password.

Change the administrator password.

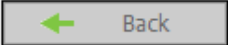
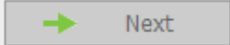
Password :

Verify Password :

☒ Use the original password

---

**Note:** If you select "Use the original password", the administrator password will not be changed.

 Back  Next

Step 3. Enter the date, time and select the time zone for the server.

- Step 3/6: Enter the date, time and time zone for this server.

Time Zone :

Date / Time:   :  :

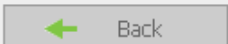
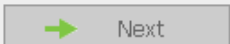
☐ Synchronize with an Internet time server automatically

Server:   (Status: --)

☒ Set the server time the same as your computer time.

---

**Tip:** Enable "Synchronize with an Internet time server automatically", the server time will be synchronized with the NTP server automatically.

 Back  Next

**Step 4. Enter the IP address, subnet mask and default gateway for the server.**

– Step 4/6: Enter the IP address, subnet mask and default gateway for this server.

☒ Obtain TCP/IP settings automatically via DHCP

☐ Use the following settings

IP Address:

Subnet Mask:



Default Gateway:

Primary DNS Server

Secondary DNS Server

---

**Tip:** If you do not need to specify the gateway IP, enter "0.0.0.0". To use a fixed IP, enter the correct DNS server IP. Otherwise, the NAS may not be able to synchronize the server time with the NTP server or send alert emails.

 Back  Next



**Note:**

1. Please contact your ISP or network administrator for the IP address of primary and secondary DNS servers. When the NAS plays the role as a terminal and needs to perform independent connection, e.g. BT download, you must enter at least one DNS server IP for proper URL connection. Otherwise, the function may not work properly.
2. If you select to obtain IP address via DHCP, there is no need to configure the primary and secondary DNS servers. You can enter "0.0.0.0" in the settings.

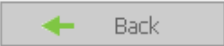
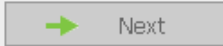
Step 5. Select the services to enable on the NAS.

– Step 5/6: Select the services to be enabled.

Network services:	<input checked="" type="checkbox"/> Microsoft Networking	<input type="checkbox"/> Apple Networking	<input type="checkbox"/> Unix/Linux NFS
File services:	<input checked="" type="checkbox"/> Web File Manager	<input checked="" type="checkbox"/> FTP Service	<input checked="" type="checkbox"/> Download Station
Multimedia services:	<input checked="" type="checkbox"/> Multimedia Station	<input type="checkbox"/> UPnP multimedia server	<input type="checkbox"/> iTunes service
Web server services:	<input type="checkbox"/> Web Server	<input type="checkbox"/> MySQL server	

---

**Tip:** You can select the network services to be enabled after the system is ready. To configure the detailed settings of the services, please go to the corresponding administration pages after finishing the quick configuration.

 Back  Next

Step 6. Select the disk configuration for your hard drives.

Select to encrypt the disk volume or not. Select “Yes” and the disk volume will be encrypted by AES 256-bit encryption. An encrypted disk volume must be unlocked after the server is turned on so that it is mounted and can be accessed normally.

**Encryption Password:** Enter the encryption password for the disk volume. The password should be 8-16 characters long.

**Use Default Value:** Check this option to use the default password. The default password is “admin”.

**Save Encryption Key:** Check this option and the encryption key is saved on the system. The server will use the key to unlock the disk volume after system startup and mount the disk automatically. If you select not to save the key, you need to enter the key to unlock the disk volume in “Device Configuration” > “Disk Volume Encryption Management” every time the system is started up.

– Step 6/6: Select the disk configuration

**Note:** The hard drive(s) has (have) been initialized. Select "Do not set disk configuration" or the drive data will be cleared.

Please select the disk configuration for the initialization.

Disk configuration: Single Disk Total available storage capacity: 1541.82 GB

You may select to use the hard drives as single disk volumes. However, when a drive failure occurs, all data will be lost.

Encrypt disk volume: Yes

Input Encryption Password: \_\_\_\_\_

Verify Encryption Password: \_\_\_\_\_

☒ Use Default Value ☒ Save Encryption Key

The hard drive(s) detected by NAS:

Disk	Model	Capacity
Drive 1	--	--
Drive 2	Seagate ST31000340AS SD15	931.51 GB
Drive 3	Seagate ST3160827AS 3.42	149.05 GB
Drive 4	Seagate ST3500320AS SD15	465.76 GB

**Tip:** All settings will be effective after confirming the changes in the last step.

 Back


 Next


Finished. The basic system settings are shown. Click "Start Installation" to begin system installation.

Finish

The changes you have made to the server are as below. Click "Start installation" to begin the quick configuration; or click "Back" to return to the previous steps to modify the settings.

Server Name :	NASBA9B4C		
Password:	The password is unchanged.		
Time Zone :	(GMT+08:00) Taipei		
Time Setting:	2008/12/24 16:23:17		
Network :	Obtain TCP/IP settings automatically via DHCP		
Primary DNS Server	0.0.0.0		
Secondary DNS Server	0.0.0.0		
Network services:	Microsoft Networking,Web File Manager,FTP Service,Download Station,Multimedia Station		
Disk configuration:	Do not set disk configuration		
Encrypt disk volume:	No		
Drive 1:	--	--	
Drive 2:	Seagate ST31000340AS SD15	931.51 GB	
Drive 3:	Seagate ST3160827AS 3.42	149.05 GB	
Drive 4:	Seagate ST3500320AS SD15	465.76 GB	

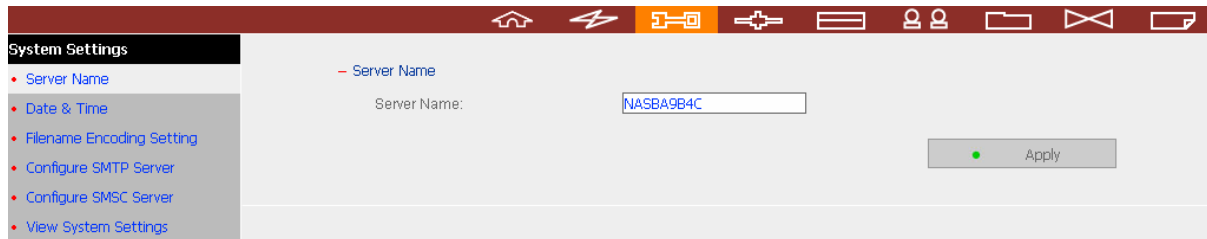
 Back

 Start installation



## 3.3 System Settings

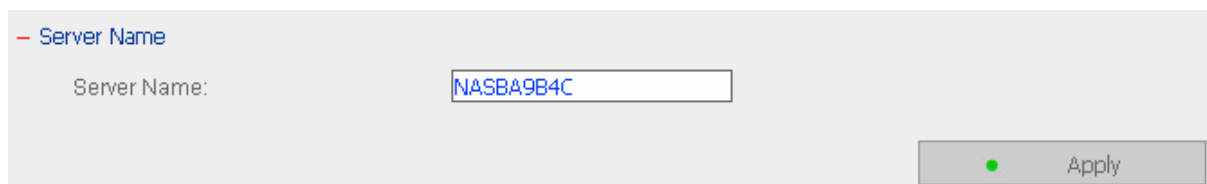
Configure the server name, date & time, and file name encoding in the System Settings.



The screenshot shows a web-based configuration interface. At the top is a dark red navigation bar with several icons. Below it is a sidebar with a black header 'System Settings' and a list of menu items: 'Server Name', 'Date & Time', 'Filename Encoding Setting', 'Configure SMTP Server', 'Configure SMSC Server', and 'View System Settings'. The 'Server Name' item is selected. The main content area has a light gray background. At the top of this area is a red minus sign followed by the text 'Server Name'. Below this is the label 'Server Name:' followed by a text input field containing the value 'NASBA9B4C'. To the right of the input field is a gray button with a green dot and the text 'Apply'.

### 3.3.1 Server Name

Please assign a unique name for this server for ease of identification within the local network. The length of server name can be up to 14 characters, which can be a combination of alphabetical letters (A-Z or a-z), numbers (0-9) and hyphens (-). The server will not accept spaces, period (.), or other symbols.



This is a close-up of the configuration field shown in the previous screenshot. It features a red minus sign and the text 'Server Name' at the top. Below is the label 'Server Name:' followed by a text input field containing the value 'NASBA9B4C'. To the right of the input field is a gray button with a green dot and the text 'Apply'.

### 3.3.2 Date & Time

Set the date, time, and time zone according to your location. If the settings are incorrect, the following problems may occur:

- ✓ When using a web browser to access or save a file, the display time of the action will be incorrect.
- ✓ The time of event log displayed will be inconsistent with the actual time when an action occurs.

– Adjust the date, time and time zone of this server

Time Zone: (GMT+08:00) Taipei ▼

Date / Time 2008/12/24 ▼ 16 ▼ : 26 ▼ : 14 ▼

☐ Synchronize with an Internet time server automatically

Server: pool.ntp.org Update now (Status: --)

Time Interval 1 day(s) ▼

☐ Set the server time the same as your computer time.

Apply

#### ✓ Synchronize with an Internet time server automatically

You can enable this option to update the date and time of the system automatically with an NTP (Network Time Protocol) server. Enter the IP address or domain name of the NTP server, e.g. time.nist.gov, time.windows.com. Then enter the time interval when the server time should be updated.



**Note:** The first time you enable NTP server, it may take several minutes to synchronize the time with the NTP server.

### 3.3.3 Filename Encoding Setting

Select the language the NAS uses to display files and directories.



**Note:** All files and directories on the NAS will be created using Unicode encoding. If your FTP clients or the OS of your PC does not support Unicode, e.g. Windows® 95/98/ME, select the language the same as your OS here in order to view the files and directories on the server properly.

- Filename Encoding Setting

Filename Encoding:

### 3.3.4 Configure SMTP Server

Configure the SMTP server for outgoing mails of this server. If your mail server requires SMTP authentication, please enter the user name and password for the mail server.

- Configure SMTP Server

SMTP Server:

Sender:

☐ Enable SMTP Authentication

    User Name :

    Password :

☒ Use SSL/ TLS secure connection

### 3.3.5 Configure SMSC Server

You can configure the SMS server settings to send SMS messages from the NAS. The default SMS service provider is Clickatell. You may also add your own SMS service provider by selecting "Add SMS Provider" on the drop down menu.

When you select "Add SMS service provider", you need to enter the name of the SMS provider and the URL template text.

**Note:** You will not be able to receive the SMS properly if the URL template text entered does not follow your SMS service provider's standard.

- SMSC Settings

You can configure the SMSC settings to send instant system alerts via the SMS service provided by the SMS provider.

SMS Service Provider

Clickatell

Clickatell

Add SMS service provider

<http://www.clickatell.com>

☐ Enable SSL Connection

SSL Port:

443

SMS Server Login Name

SMS Server Login Password

SMS Server API\_ID

Apply

### 3.3.6 View System Settings

You can view all current system settings, e.g. server name, on this page.


[View System Settings](#)

Server Name	
Server Name	NASBA9B4C

Date & Time	
Date	December 24, 2008
Time	4:26:59 PM
Time Zone	(GMT+08:00) Taipei

Filename Encoding	
Code Page	English (437)

System Information	
Version	2.1.0 Build 1215T

 OK

## 3.4 Network Settings

You can configure network settings in this section and enable several powerful applications of the NAS, e.g. Multimedia Station, Download Station, and Web Server.

### 3.4.1 TCP/ IP Configuration

The NAS provides two ports that you can configure failover, load balancing, or standalone functions. When you use these functions, make sure both LAN ports are connected to the network.

The screenshot displays the 'Network Settings' window with a sidebar on the left containing a list of services: TCP/IP Configuration, Microsoft Networking, Apple Networking, NFS Service, Web File Manager, FTP Service, Multimedia Station, iTunes Service, Download Station, Web Server, DDNS Service, MySQL Server, Surveillance Station, System Port Management, and View Network Settings. The main panel is titled 'TCP/IP Configuration' and includes a sub-header 'Configuration of Network Interfaces' with three radio buttons: Failover (selected), Load balancing, and Standalone. Below this, the 'Failover' tab is active, showing a configuration box with the following settings: Network transfer rate set to 'Auto-negotiation'; 'Obtain IP address settings automatically via DHCP' selected; Fixed IP Address set to 169.254.100.100; Subnet Mask set to 255.255.0.0; Default Gateway set to 169.254.100.100; Primary and Secondary DNS Servers both set to 0.0.0.0; 'Enable DHCP Server' unchecked; Start IP Address set to 169.254.1.100; End IP Address set to 169.254.1.200; Lease Time set to 1 Day(s) and 0 Hour(s); Current connection status showing 'Connection speed: 100 Mbps, MTU: 1500 Bytes, LAN1:Down, LAN2:Up'; Jumbo Frame Setting (MTU) with explanatory text and a dropdown menu set to 'Disable Jumbo Frame, MTU value is 1500 bytes'. An 'Apply' button is located at the bottom right of the configuration box.

## Configuration of Network Interfaces

- **Failover (Default)**

Failover refers to the capability of switching over the network transfer port to the redundant port automatically when the primary one fails due to hardware or connection error to avoid network disconnection. When the primary network port resumes to work, the network transfer will be switched back to that port automatically.

The screenshot shows a configuration window titled "Failover". It contains several sections for network configuration:

- Network transfer rate:** A dropdown menu set to "Auto-negotiation".
- IP Addressing:** Two radio buttons. "Obtain IP address settings automatically via DHCP" is unselected, and "Use static IP address" is selected.
- Static IP Settings:**
  - Fixed IP Address:** 172 . 17 . 21 . 122
  - Subnet Mask:** 255 . 255 . 254 . 0
  - Default Gateway:** 172 . 17 . 20 . 1
- DNS Settings:**
  - Primary DNS Server:** 10 . 8 . 2 . 11
  - Secondary DNS Server:** 0 . 0 . 0 . 0
- DHCP Server Settings:** An unchecked checkbox labeled "Enable DHCP Server". Below it are fields for:
  - Start IP Address:** 172 . 17 . 1 . 100
  - End IP Address:** 172 . 17 . 1 . 200
  - Lease Time:** 1 Day(s) 0 Hour(s)

- **Load balancing**

Load balancing enables the network resources to spread between two or more network interfaces to optimize network transfer and enhance system performance. It operates on layer 3 protocol (IP, NCP IPX) only. Multicast/ broadcast and other non-routable protocols, e.g. NetBEUI, can only be transferred via the main network port.

**Note:** To optimize the network transfer speed of the NAS in load balancing mode, please use a managed Ethernet switch and enable 802.3ad (or link aggregation) on the ports of the switch that the Giga LAN ports of the NAS are connected to.

Load balancing

Network transfer rate Auto-negotiation ▼

☐ Obtain IP address settings automatically via DHCP

☒ Use static IP address

Fixed IP Address 172 . 17 . 21 . 122

Subnet Mask 255 . 255 ▼ . 254 ▼ . 0 ▼

Default Gateway 172 . 17 . 20 . 1

Primary DNS Server 10 . 8 . 2 . 11

Secondary DNS Server 0 . 0 . 0 . 0

☐ Enable DHCP Server

Start IP Address 172 . 17 . 1 . 100

End IP Address 172 . 17 . 1 . 200

Lease Time 1 Day(s) 0 Hour(s)



- **Standalone**

The standalone option allows you to assign different IP settings for each network port. The NAS can be accessed by different workgroups in two different subnets. However, when this function is enabled, failover does not work. You can only enable DHCP server for the primary network port (LAN 1).

The screenshot shows the network configuration interface for LAN 1. The interface is divided into two tabs: LAN 1 (selected) and LAN 2. The LAN 1 tab contains the following settings:

- Network transfer rate:** A dropdown menu set to "Auto-negotiation".
- Obtain IP address settings automatically via DHCP:** A radio button that is selected.
- Use static IP address:** A radio button that is unselected.
- Fixed IP Address:** Four input fields showing "169", "254", "100", and "100".
- Subnet Mask:** Four input fields showing "255", "255", "0", and "0".
- Default Gateway:** Four input fields showing "169", "254", "100", and "100".
- Primary DNS Server:** Four input fields showing "10", "8", "2", and "11".
- Secondary DNS Server:** Four input fields showing "0", "0", "0", and "0".
- Enable DHCP Server:** A checkbox that is unselected.
- Start IP Address:** Four input fields showing "172", "17", "1", and "100".
- End IP Address:** Four input fields showing "172", "17", "1", and "200".
- Lease Time:** Two input fields showing "1" and "0", with labels "Day(s)" and "Hour(s)".

### Network Transfer Rate

you can select auto-negotiation (default), 1000 Mbps, or 100 Mbps. It is recommended to use the default setting that the server will determine network speed automatically.

### Obtain IP address settings automatically via DHCP

If your network supports DHCP, the NAS will use DHCP protocol to retrieve the IP address and related information automatically.

### Use static IP address

To use fixed IP address for network connection, enter fixed IP address, subnet mask, and default gateway.

**Primary DNS Server:** Enter the IP address of primary DNS server that provides DNS

service for the NAS in external network.

**Secondary DNS Server:** Enter the IP address of secondary DNS server that provides DNS service for the NAS in external network.



**Note:**

1. Please contact your ISP or network administrator for the IP address of primary and secondary DNS servers. When the NAS plays the role as a terminal and needs to perform independent connection, e.g. BT download, you must enter at least one DNS server IP for proper URL connection. Otherwise, the function may not work properly.
2. If you select to obtain IP address via DHCP, there is no need to configure the primary and secondary DNS servers. You can enter "0.0.0.0" in the settings.

### **Enable DHCP Server**

If no DHCP is available in the LAN where the NAS locates, you can enable this function to enable the NAS as a DHCP server and allocate dynamic IP address to DHCP clients in LAN.

You can set the range of IP addresses allocated by DHCP server and the lease time. Lease time refers to time that IP address is leased to the clients by DHCP server. When the time expires, the client has to acquire an IP address again.

For example, to establish a DLNA network, and share the multimedia files on the NAS to DLNA DMP via UPnP while there is no NAT gateway that supports DHCP server, you can enable DHCP server of the NAS. The NAS will allocate dynamic IP address to DMP or other clients automatically and set up a local network.



**Note:** If there is an existing DHCP server in your LAN, do not enable this function. Otherwise, there will be IP address allocation and network access errors.

## **Jumbo Frame Settings (MTU)**

"Jumbo Frames" refer to Ethernet frames that are larger than 1500 bytes. It is designed to enhance Ethernet networking throughput and reduce the CPU utilization of large file transfers by enabling more efficient larger payloads per packet.

Maximum Transmission Unit (MTU) refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can transmit.

The NAS uses standard Ethernet frames: 1500 bytes by default. If your network appliances support Jumbo Frame setting, select the appropriate MTU value for your network environment. The NAS supports 4074, 7418, and 9000 bytes for MTU.



Note: Jumbo Frame setting is valid in Gigabit network environment only. Besides, all network appliances connected must enable Jumbo Frame and use the same MTU value.

### 3.4.2 Microsoft Networking

- Microsoft Networking

☒ Enable file service for Microsoft networking

☒ Standalone Server  
☐ AD Domain Member

Server Description: NAS Server

Workgroup: NAS

AD Server Name:

Domain Name:

Domain Username:

Password:

☐ Enable WINS server  
☒ Use the specified WINS server

WINS server IP address: 0 . 0 . 0 . 0

☐ Domain Master

Apply

**Enable file service for Microsoft networking:** If you are using Microsoft® Windows® OS, enable this service to access the files on network share folders. Assign a workgroup name.

✓ **Standalone Server**

Use local users for user authentication.

✓ **AD Domain Member**

The NAS supports Windows 2003 AD (Active Directory) to provide quick and direct import of user accounts to the existing AD server available in your network. This function helps you to save time and effort on creating user accounts and passwords and lowers IT maintenance cost by automatic configuration procedure.

➤ **Server Description**

Describe the NAS for users to identify the server. To use the NAS on the Microsoft Windows OS, you must enable Microsoft Network Services.

➤ **Workgroup**

Specify the workgroup the NAS belongs to. The workgroup is a computer group unit in Microsoft Windows network for network sharing.

➤ **AD Server Name**

Enter the name of the AD server when AD domain is selected for authentication.

➤ **Domain Name**

The name of Microsoft domain. When you select AD domain, you must enter the domain name, the login user name, and the password.

Please refer to Chapter 11 for the information of AD authentication.

✓ **WINS server**

If the local network has a WINS server installed, specify the IP address. The NAS will automatically register its name and IP address with WINS service. If you have a WINS server in your network and want to use this server, enter the WINS server IP.

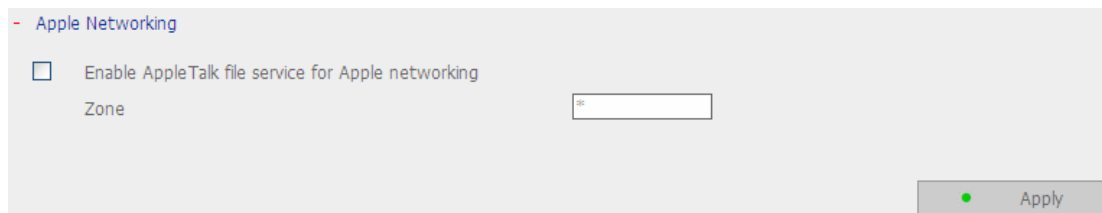
✓ **Domain Master**

There is a unique Domain Master Browser for collecting and recording resources and services available for each PC in the network or workgroup of Windows. When you find the waiting time for accessing Network Neighborhood too long, it may be caused by failure of an existing master browser, or there is no master browser in the network.

If there is no master browser in your network, you can check the box Domain Master in this section to configure the NAS as the master browser to enhance the speed of accessing information on Network Neighborhood.

### 3.4.3 Apple Networking

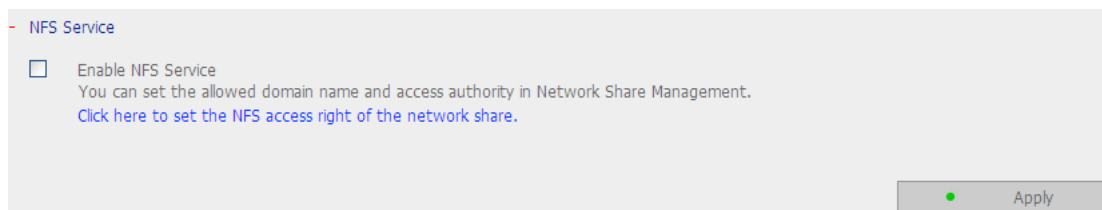
To use the NAS on Apple Mac operating system, enable AppleTalk network support. If your AppleTalk network uses extended networks, and is assigned with multiple zones, assign a zone name to the NAS. If you do not want to assign a network zone, enter an asterisk (\*) to use the default setting. **This setting is disabled by default.**



The screenshot shows the 'Apple Networking' configuration panel. It has a title bar with a minus sign and the text 'Apple Networking'. Below the title bar, there is a checkbox labeled 'Enable AppleTalk file service for Apple networking'. To the right of the checkbox is a text input field labeled 'Zone' with an asterisk (\*) inside. At the bottom right of the panel is a green status indicator and an 'Apply' button.

### 3.4.4 NFS Service

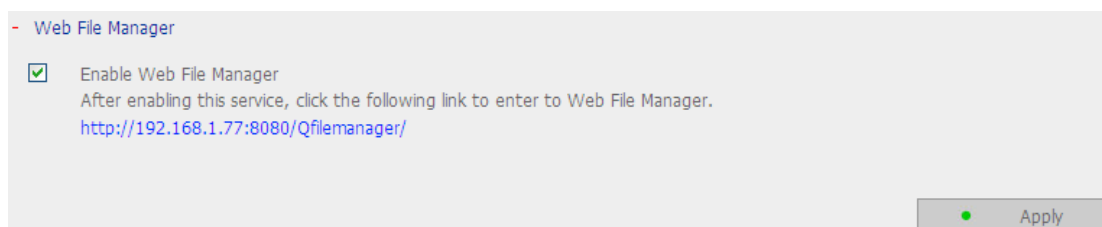
After enabling this service, you can click here to set up the Network access authority to configure the settings. For the information of connecting to the NAS via NFS on Linux, please refer to Chapter 12.



The screenshot shows the 'NFS Service' configuration panel. It has a title bar with a minus sign and the text 'NFS Service'. Below the title bar, there is a checkbox labeled 'Enable NFS Service'. To the right of the checkbox, there is a paragraph of text: 'You can set the allowed domain name and access authority in Network Share Management. Click here to set the NFS access right of the network share.' At the bottom right of the panel is a green status indicator and an 'Apply' button.

### 3.4.5 Web File Manager

To access files on the NAS via web browser, enable Web File Manager. If the NAS is connected to the Internet and uses a valid IP address, you can access files on the server by web browser from anywhere. For more information, please refer to Chapter 9. The NAS supports SSL secure login. You can select SSL login on the NAS administration page and login Web File Manager via https; or enter https://NAS IP:8080/Qfilemanager/ in the browser.



The screenshot shows the 'Web File Manager' configuration panel. It has a title bar with a minus sign and the text 'Web File Manager'. Below the title bar, there is a checked checkbox labeled 'Enable Web File Manager'. To the right of the checkbox, there is a paragraph of text: 'After enabling this service, click the following link to enter to Web File Manager. http://192.168.1.77:8080/Qfilemanager/'. At the bottom right of the panel is a green status indicator and an 'Apply' button.

### 3.4.6 FTP Service

When you enable FTP service, you can define the port number for the service and maximum number of users connected to the FTP at the same time.

FTP Service

☒ Enable FTP Service

Protocol type:

☒ FTP (standard)☐ FTP with SSL/TLS (Explicit)

Port Number

21

Unicode Support

☐ Yes ☒ No

Enable Anonymous

☐ Yes ☒ No

Passive FTP Port Range

☒ Use the default port range (55536 - 56559)☐ Define port range: 

55536

 - 

56559

☐ Respond with external IP address for passive FTP connection request

External IP address:  (Detect the IP address automatically if this blank is left empty)

Maximum number of all FTP connections: 

30

Maximum number of connections for a single account

10

☐ Enable FTP transfer limitation(0 means unlimited)

Single connection: Maximum download rate (KB/s): 

0

 KB/s,  
Maximum upload rate (KB/s): 

0

 KB/s

Note: If your FTP client does not support Unicode, please select "No" for Unicode Support and select a supported filename encoding from **Filename Encoding Setting** under **System Settings** so that the folders and files on FTP can be properly shown.

Apply

✓ **Select Protocol Type**

Select to use standard FTP connection or SSL/TLS encrypted FTP. Select the corresponding protocol type in your client FTP software to ensure successful connection.

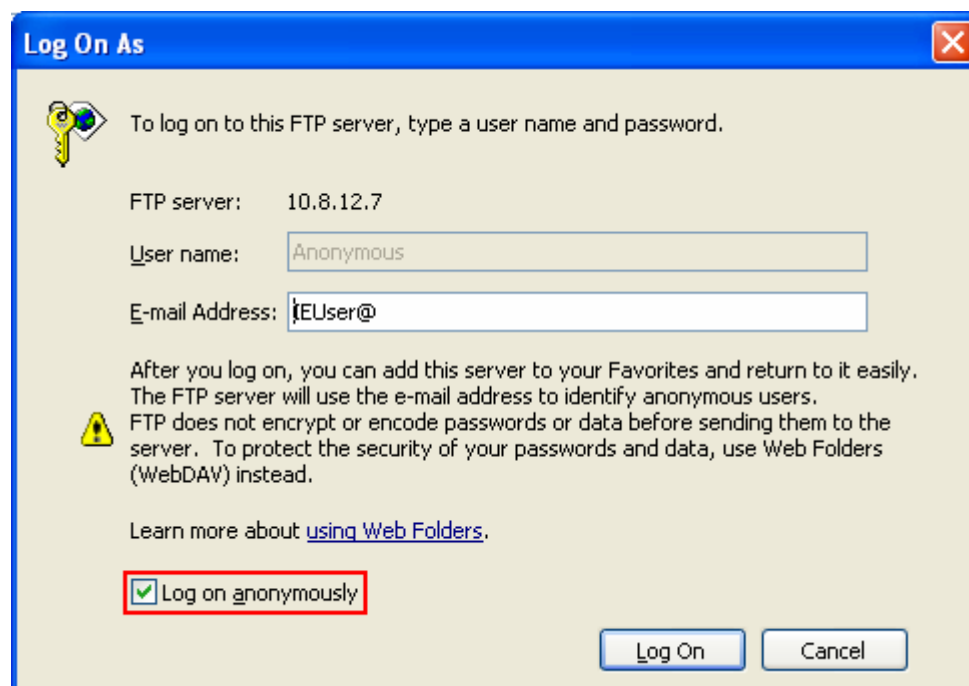
✓ **Unicode Support**

Select to enable or disable Unicode Support. The default setting is No. Since most FTP clients do not support Unicode currently, it is recommended that you disable Unicode support here and select the language the same as your OS in "System

Settings—Encoding Setting” page so that the folders and files on FTP can be properly shown (please refer to Chapter 3.3.3). If your FTP client supports Unicode, make sure you have enabled Unicode support for both your client and the NAS.

✓ **Enable Anonymous**

Enable this option to allow the users to access the NAS anonymously by FTP.



✓ **Passive FTP Port Range**

You can use the default port range (55536-56559) or define a port range larger than 1024. When using this function, please make sure you have opened the configured port range on your router or firewall.

✓ **Respond with external IP address for passive FTP connection request**

When passive FTP connection is in use and the FTP server is configured under a router, if the remote computer cannot connect to the FTP server via WAN, you can enable this function. By enabling this function, the FTP service replies the manually specified IP address or automatically detects the external IP address so that the remote computer can connect to the FTP server successfully.

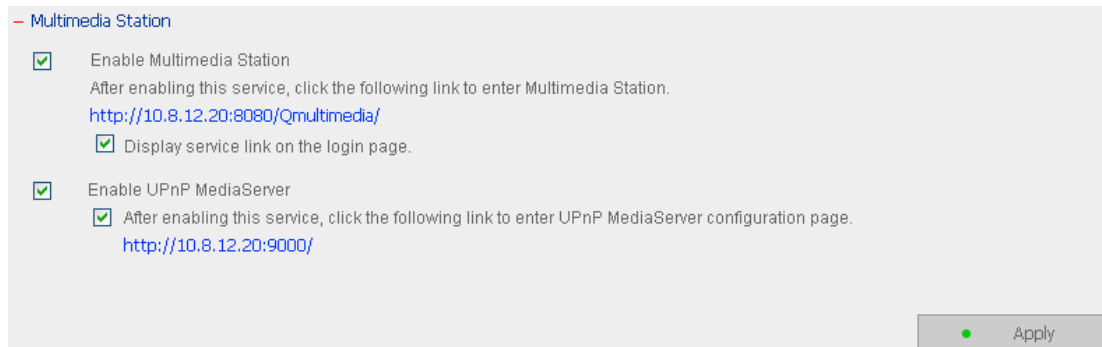
✓ **FTP Transfer Limitation**

You can configure the maximum number of all FTP connections, maximum connections of a single account and the maximum upload/ download rates of a single connection.



### 3.4.7 Multimedia Station

To share photos, music or video files on the NAS over the network, enable Multimedia Station. For further information of Multimedia Station, iTunes service and UPnP Media Server, please refer to Chapter 5.



— Multimedia Station

☒ Enable Multimedia Station  
After enabling this service, click the following link to enter Multimedia Station.  
<http://10.8.12.20:8080/Qmultimedia/>

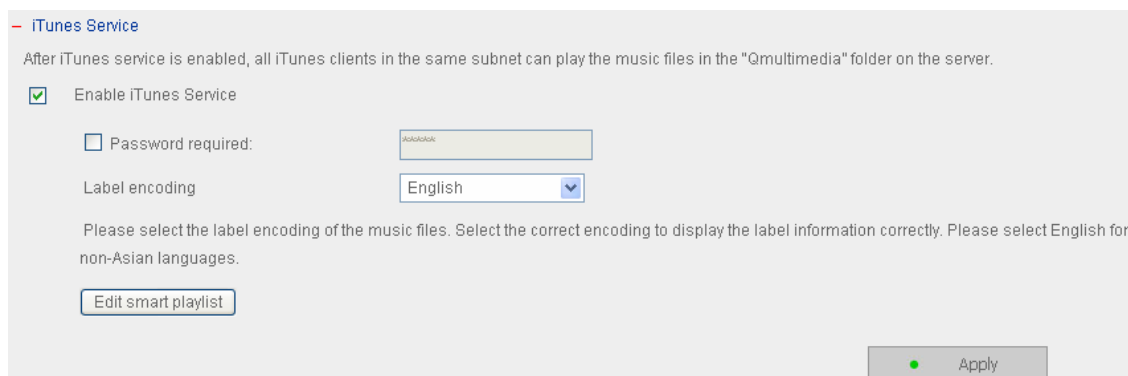
☒ Display service link on the login page.

☒ Enable UPnP MediaServer  
☒ After enabling this service, click the following link to enter UPnP MediaServer configuration page.  
<http://10.8.12.20:9000/>

● Apply

### 3.4.8 iTunes Service

By enabling the iTunes service, the NAS shares the mp3 files in the Qmultimedia folder to all the iTunes clients available in the same subnet. The clients can automatically detect, browse, and play the music files in the NAS. For further details, please refer to Chapter 5.2.



— iTunes Service

After iTunes service is enabled, all iTunes clients in the same subnet can play the music files in the "Qmultimedia" folder on the server.

☒ Enable iTunes Service

☐ Password required:

Label encoding:

Please select the label encoding of the music files. Select the correct encoding to display the label information correctly. Please select English for non-Asian languages.

[Edit smart playlist](#)

● Apply

### 3.4.9 Download Station

The NAS supports BT, HTTP and FTP download independent of PC/notebook. To use the download function of the NAS, please enable Download Station. For further information, please refer to Chapter 6.

Download Station

☒

Enable Download Station

After enabling this service, click the following link to enter to Download Station.

<http://10.8.12.20:8080/Qdownload/>

☒

Display service link on the login page.

Apply



**Warning:** Please be warned against illegal downloading of copyrighted materials. The Download Station functionality is provided for downloading authorized files only. Downloading or distribution of unauthorized materials may result in severe civil and criminal penalty. Users are subject to the restrictions of the copyright laws and should accept all the consequences.

### 3.4.10 Web Server

You can publish your own server by enabling Web Server function of the NAS. Enter the port number for web server service, the default number is 80. For further information, please refer to Chapter 7.

Web Server

After enabling this function, you can upload the webpage files to Qweb network share to publish your website.

☒

Enable Web Server

View version

Port Number

80

After enabling this service, click the following link to enter to Web Server.

<http://172.17.21.123:80/>

The built-in web page applications of the system are as below (make sure you have enabled MySQL server and Web server)

- Click the link on the right to enter Joomla content management system

<http://172.17.21.123:80/Joomla/>

register\_globals

☐ On

☒ Off

●

Apply

☐

php.ini Maintenance

The file **php.ini** is the system configuration file of Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended to use the system default setting.

#### Configure register\_globals

Select to enable or disable register\_globals. The setting is disabled by default. When the web program asks to enable php register\_globals, please enable this option. However, for system security concerns, it is recommended to disable this option.

#### php.ini Maintenance

☒

php.ini Maintenance

Please select...

Please select...

Upload

Edit

Restore

The file **php.ini** is the system configuration file of Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended to use the system default setting.

Check the box "php.ini Maintenance" to select to upload, edit or restore php.ini.

Edit: Edit the current php.ini file.

Upload: Upload a new php.ini file to replace the current file.

Restore: Restore the php.ini file to system default.



**Note:** To use PHP mail() function, you can go to System Settings/ Configure SMTP Server to configure the SMTP server settings.

### 3.4.11 DDNS Service

- DDNS Service

After enabling DDNS Service, you can connect to this server by domain name.

☒ Enable Dynamic DNS Service

Select DDNS server:

Enter the account information you registered with the DDNS provider:

User Name:

Password:

Host Name:

☐ Check the external IP address automatically

( External IP : 219.85.63.13 )

---

Note: When the external IP is changed, the system updates the information with the DDNS provider.

To set up a server on the Internet and enable users to access it easily, a fixed and easy-to-remember host name is often required. However, if ISP provides only dynamic IP address, the IP address of the server will change from time to time and is difficult to recall. You can enable DDNS service to solve the problem.

After enabling DDNS service of the NAS, whenever the NAS restarts or the IP address is changed, the NAS will notify DDNS provider immediately to record the new IP address. When the user tries to connect the NAS via the host name, DDNS will transfer the recorded IP address to the user.

#### Enable and configure DDNS of the NAS:

Before using DDNS service, please register a host name from the DDNS provider\*. The NAS supports the DDNS providers: members.dyndns.org, update.ods.org, members.dhs.org, www.dyns.cx, www.3322.org, www.no-ip.com.

Enable Dynamic DNS Service, and select DDNS server. Then enter the user name, password, and hostname.

\* For the information of DDNS service registration, please refer to the website of the DDNS providers.

### 3.4.12 MySQL Server

MySQL Server

☒ Enable MySQL Server

You can enable MySQL server as the website database.

☒ Enable TCP/IP Networking

Enable this option to allow remote connection of MySQL server.

Port Number

3306

The built-in web page applications of the system are as below (make sure you have enabled MySQL server and Web server)

- Click the link on the right to enter phpMyAdmin database management system  
<http://172.17.21.123:80/phpMyAdmin/>

☐ Database Maintenance

You can reset the database password or re-initialize the database.

Apply

You can enable MySQL Server as the website database.

#### Enable remote connection of MySQL Server

You can enable this option to configure the NAS as a database server of another web server in remote site through Internet connection. When you disable this option, your MySQL Server will only be configured as local database server for the web server. After enabling remote connection, please assign a port for the remote connection service of MySQL server. The default port is 3306.

After the first-time installation of the NAS, a folder phpMyAdmin is created in the Qweb network folder. You can enter `http://NAS IP/phpMyAdmin/` in the web browser to enter the phpMyAdmin page and manage the MySQL database.



**Note:**

1. Please do not delete the phpMyAdmin folder. You can rename this folder but the link on the MySQL Server page will not be updated. To access the renamed folder, you can enter the link `http://NAS IP/renamed folder` in the web browser.
2. The phpMyAdmin folder is created after the first-time installation. When you update the firmware, the folder remains unchanged.

### Database Maintenance

Check the box **Database Maintenance** to reset the database password or initialize the database.



**Database Maintenance**

You can reset the database password or re-initialize the database.

Reset root password

Execute

Re-initialize database

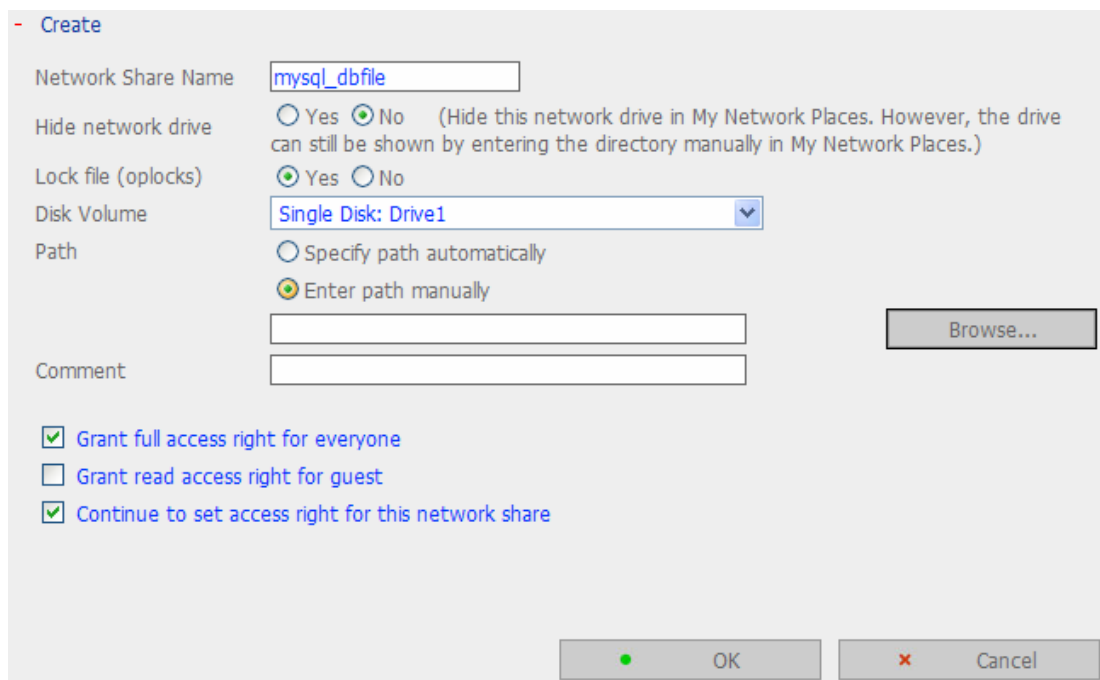
Execute

Reset root password: Execute this function to reset the password of MySQL root as **"admin"**.

Re-initialize database: Execute this function to delete all the data on MySQL database.

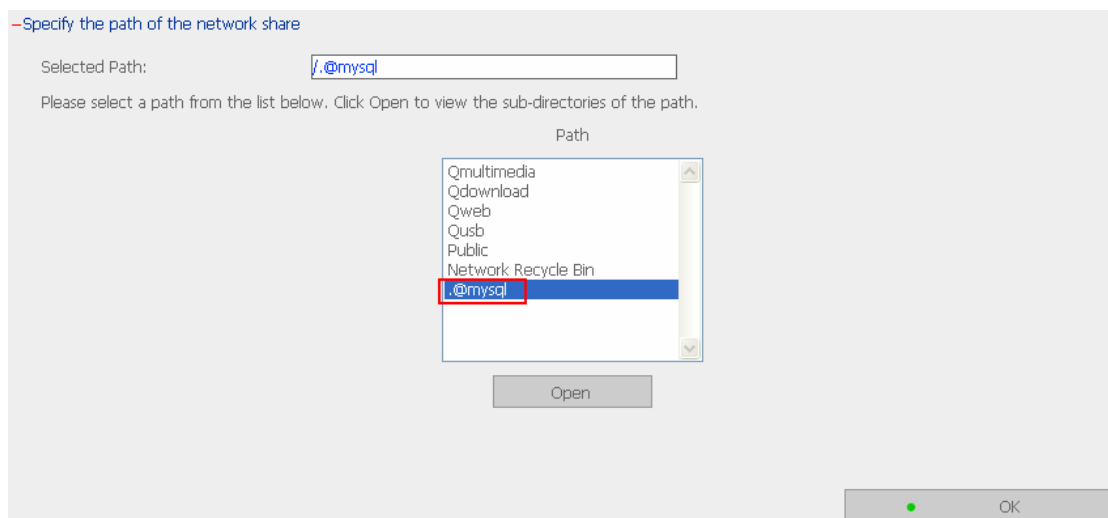
## Description: File location of MySQL database

1. Create a network share in **Network Share Management**.
2. Enter the network share name and select "Enter path manually". Then click "Browse..."



The screenshot shows the 'Create' dialog box for setting up a network share. The 'Network Share Name' field is filled with 'mysql\_dbfile'. Under the 'Path' section, the 'Enter path manually' radio button is selected. A 'Browse...' button is visible to the right of the path input field. At the bottom, there are three checkboxes: 'Grant full access right for everyone' (checked), 'Grant read access right for guest' (unchecked), and 'Continue to set access right for this network share' (checked). 'OK' and 'Cancel' buttons are at the bottom right.

3. Select .@mysql and click "OK". After the network share is created, configure the access right. The network share name configured in the above step is the file location of MySQL database.



The screenshot shows the 'Specify the path of the network share' dialog box. The 'Selected Path' field contains './@mysql'. Below the text 'Please select a path from the list below. Click Open to view the sub-directories of the path.', there is a list box titled 'Path' containing several system folders. The folder './@mysql' is highlighted with a blue selection bar and a red rectangular box. An 'Open' button is located below the list box. At the bottom right, there is an 'OK' button.



### 3.4.13 Surveillance Station

The Surveillance Station enables you to monitor and record the live video of up to **2** network cameras available on the network (LAN or WAN). To use this function, enable "Surveillance Station" in the "Network Settings" page.

Click the link or enter the URL "http://NAS IP:8080/Qrecordings" in the web browser or click "Surveillance Station" on the login page to enter the Surveillance Station.

**Note:** The Surveillance Station is only supported on IE browser 6.0 or later.

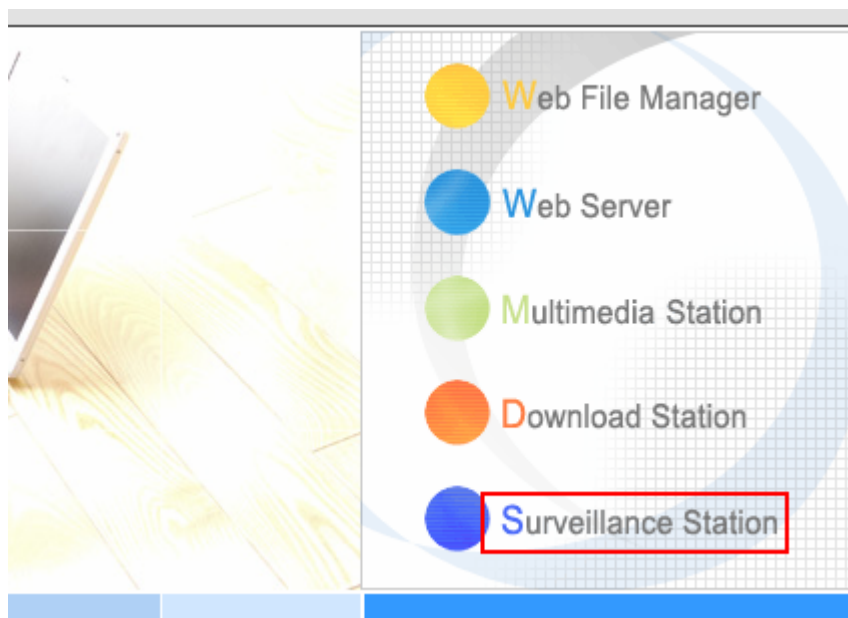
- Surveillance Station

☒ Enable Surveillance Station  
After enabling this service, click the following link to enter Surveillance Station. <http://172.17.21.123:8080/Qrecordings/>

☐ Display service link on the login page.

**Note: To use Surveillance Station , please update the system firmware with the image file enclosed in the product CD or download the latest system firmware from QNAP website: <http://www.qnap.com>**

Apply



To set up your network surveillance system by NAS, follow the steps below:

1. Plan your home network topology
2. Set up the IP Cameras
3. Configure the camera settings on NAS
4. Configure your NAT router (for remote monitoring over the Internet)

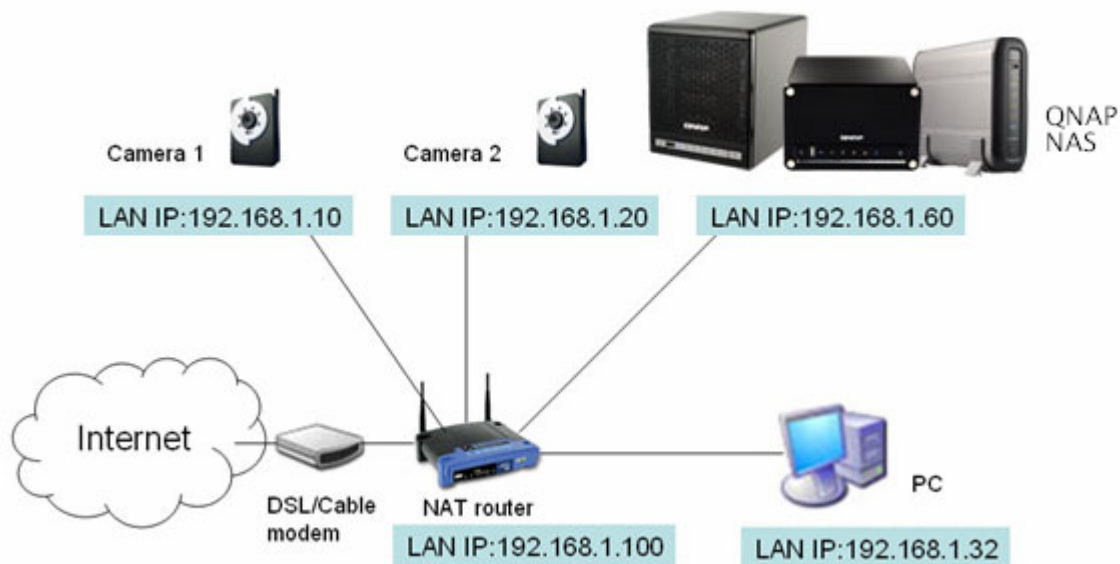
### 1. Plan your home network topology

Write down your plan of the home network before starting to set up the surveillance system. Consider the following when doing so:

- i. The IP address of NAS
- ii. The IP address of the cameras

Your computer, the NAS, and the IP cameras should be installed to the same router in LAN. Assign fixed IP addresses to the NAS and the IP cameras. For example,

- The LAN IP of the home router: 192.168.1.100
- Camera 1 IP: 192.168.1.10 (fixed IP)
- Camera 2 IP: 192.168.1.20 (fixed IP)
- NAS IP: 192.168.1.60 (fixed IP)



## 2. Set up the IP Cameras

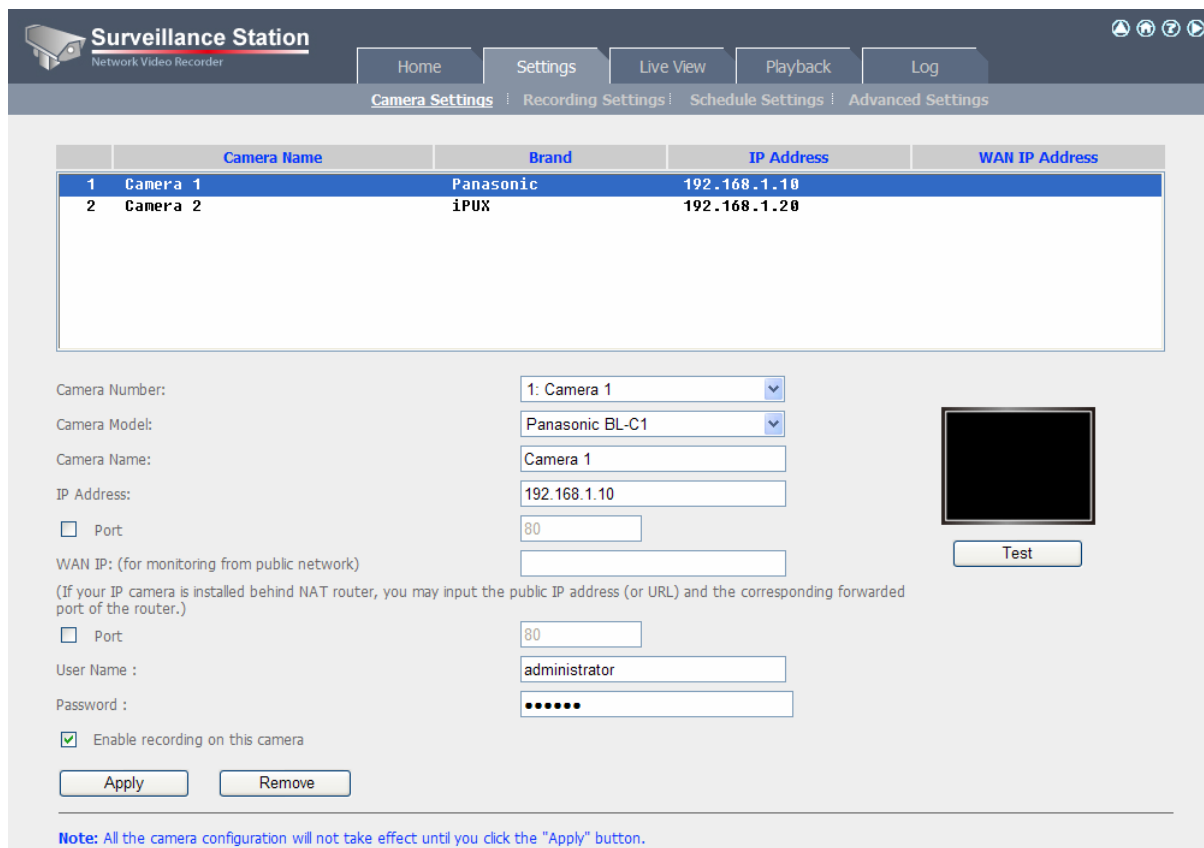
In this example, two IP cameras will be installed. Connect the IP cameras to your home network. Then set the IP address of the cameras so that they are in the same LAN as the computer. Login the configuration page of the Camera 1 by IE browser. Enter the IP address of the first camera as 192.168.1.10. The default gateway should be set as the LAN IP of the router (192.168.1.100 in this example). Then configure the IP address of the second camera as 192.168.1.20.

Some cameras provide a utility for IP configuration. You may refer to the user manual of the cameras for further details.

**\* Please refer to [www.qnap.com](http://www.qnap.com) for the supported network camera list.**

## 3. Configure the camera settings on NAS

Login the Surveillance Station by IE browser to configure the IP cameras. Go to "Settings>Camera Settings" page. Enter the camera information, e.g. name, model, and IP address.



	Camera Name	Brand	IP Address	WAN IP Address
1	Camera 1	Panasonic	192.168.1.10	
2	Camera 2	iPUX	192.168.1.20	

Camera Number: 1: Camera 1

Camera Model: Panasonic BL-C1

Camera Name: Camera 1

IP Address: 192.168.1.10

☐ Port: 80

WAN IP: (for monitoring from public network)  
(If your IP camera is installed behind NAT router, you may input the public IP address (or URL) and the corresponding forwarded port of the router.)

☐ Port: 80

User Name : administrator

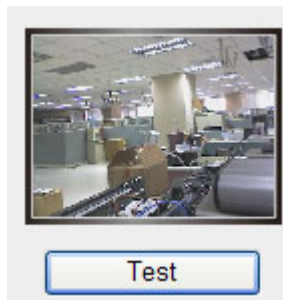
Password : .....

☒ Enable recording on this camera

Apply Remove

**Note:** All the camera configuration will not take effect until you click the "Apply" button.

Click "Test" on the right to ensure the connection to the IP camera is successful.




You may enable continuous recording by checking the option "Enable recording on this camera".

If your camera supports audio recording, you may enable the option in "Recording Settings" page. Click "Apply" to save the changes.

Camera Number:	2: Camera 2
Video Compression:	Motion JPEG
Resolution:	QVGA
Frame Rate:	20
Quality:	Normal
<input checked="" type="checkbox"/> Enable audio recording on this camera	
Estimated Storage Space for Recording: 6760 GB	
Apply	

Configure the settings of Camera 2 following the above steps.

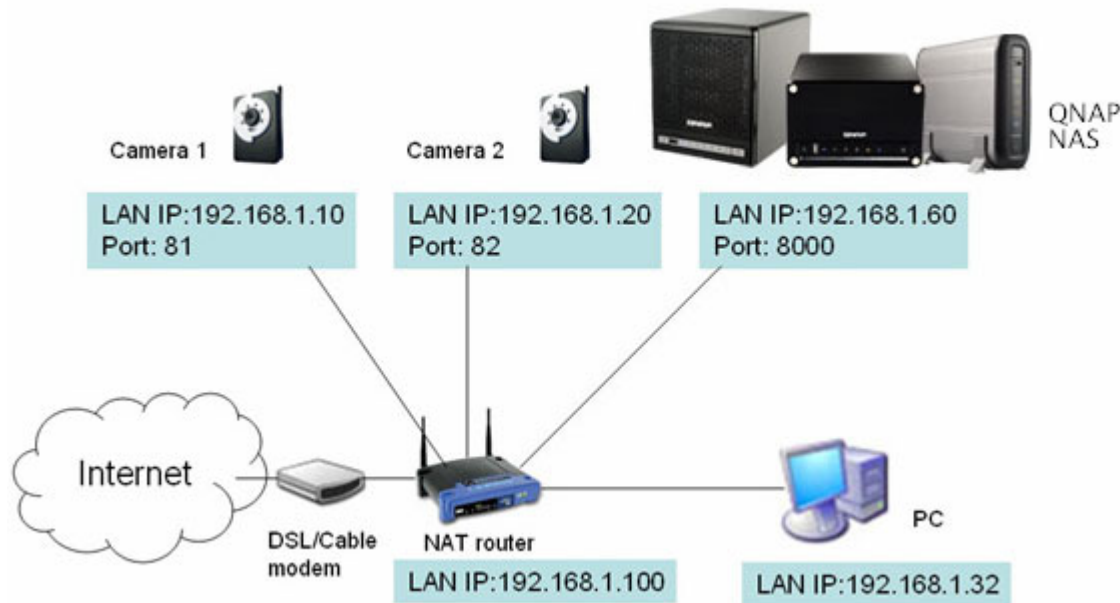
After you have added the network cameras to NAS, go to the "Live View" page. The first time you access this page by IE browser, you have to install the ActiveX control in order to view the images of Camera 1 and Camera 2. You can start to use the monitoring and recording functions of the Surveillance Station.

To use other functions of the Surveillance Station such as motion detection recording, schedule recording, and video playback, please refer to the online help .



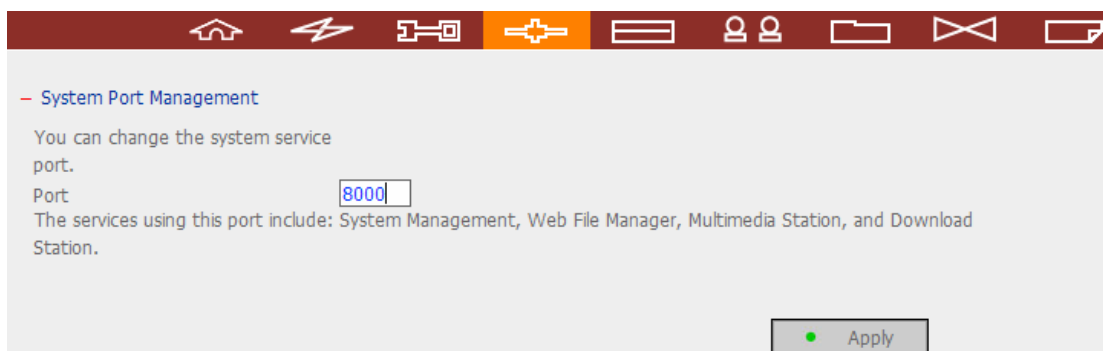
#### 4. Configure your NAT router (for remote monitoring over the Internet)

To view the monitoring video and access the NAS remotely, you need to change the network settings by forwarding different ports to the corresponding LAN IP on your NAT router.



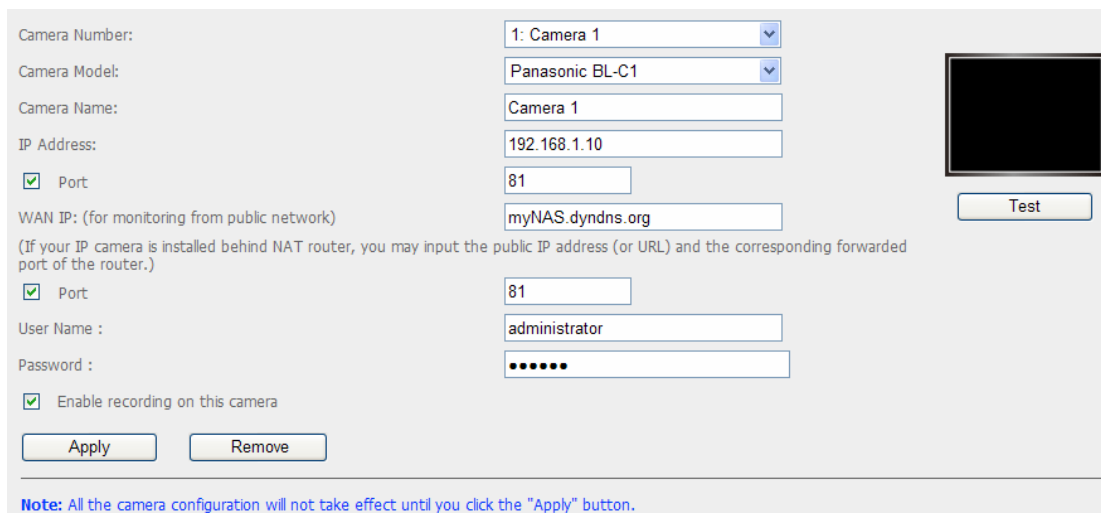
Change the port settings of NAS and IP cameras

The default HTTP port of NAS is 8080. In this example, the port is changed to 8000. Therefore, you have to access the NAS via **http://NAS IP:8000** after applying the settings.



Then login the network settings page of the IP cameras. Change the HTTP port of Camera 1 from 80 to 81. Then change the port for Camera 2 from 80 to 82.

Next, login Surveillance Station. Go to "Settings>Camera Settings". Enter the port numbers of Camera 1 and Camera 2 as 192.168.1.10 **port 81** and 192.168.1.20 **port 82** respectively. Enter the login name and password for both cameras. Besides, enter the WAN IP address (or your domain address in public network, e.g. MyNAS.dyndns.org) and the port on the WAN side for the connection from Internet. After finishing the settings, click "Test" to ensure successful connection to the cameras.



Camera Number: 1: Camera 1

Camera Model: Panasonic BL-C1

Camera Name: Camera 1

IP Address: 192.168.1.10

☒ Port 81

WAN IP: (for monitoring from public network) myNAS.dyndns.org

(If your IP camera is installed behind NAT router, you may input the public IP address (or URL) and the corresponding forwarded port of the router.)

☒ Port 81

User Name : administrator

Password : .....

☒ Enable recording on this camera

Apply Remove

**Note:** All the camera configuration will not take effect until you click the "Apply" button.

Go to the configuration page of your router and configure the port forwarding as below:

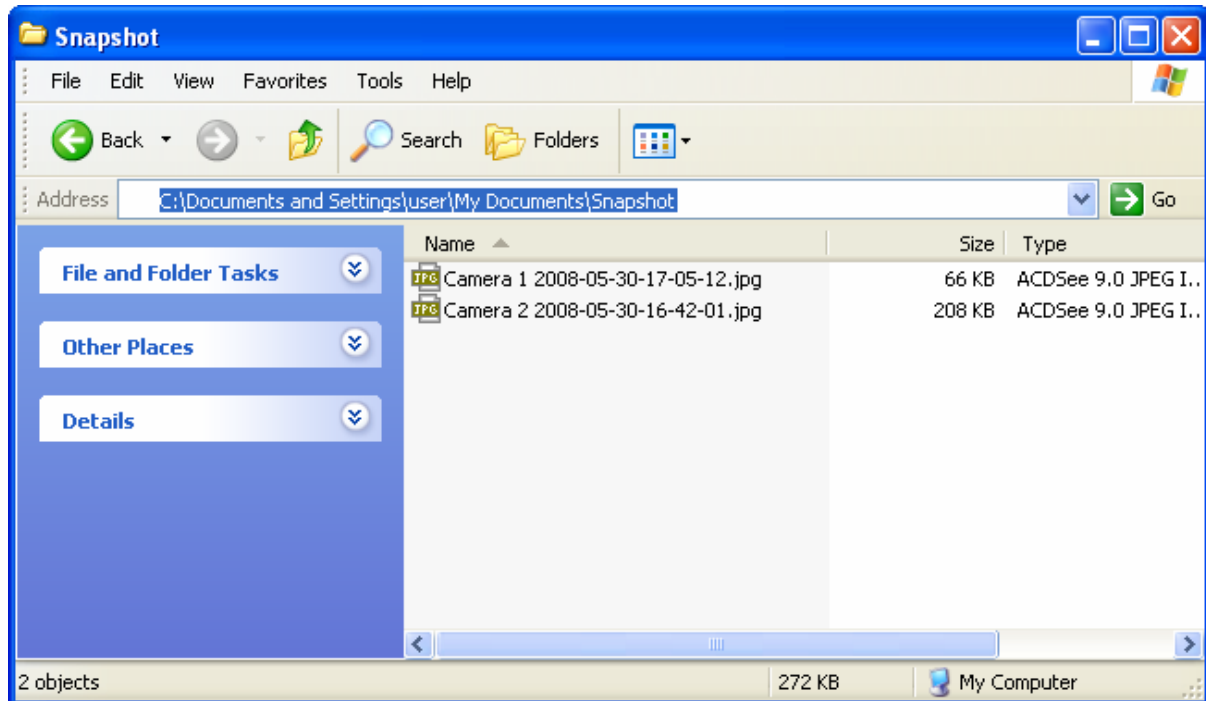
- Forward Port 8000 to NAS LAN IP: 192.168.1.60
- Forward Port 81 to Camera 1's LAN IP: 192.168.1.10
- Forward Port 82 to Camera 2's LAN IP: 192.168.1.20

**Note:** When you change the port settings, make sure remote access is allowed. For example, if your office network blocks port 8000, you will not be able to access your NAS from the office.

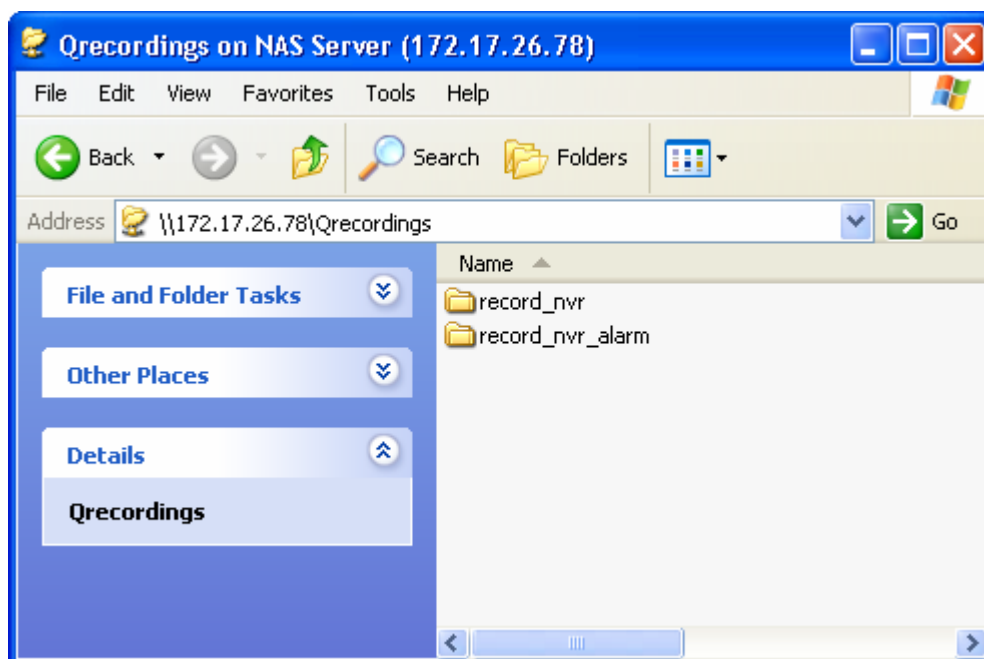
After you have configured the port forwarding and router settings, you can start to use the Surveillance Station for remote monitoring over the Internet.

## Access the snapshots and video recordings of Surveillance Station

All snapshots taken are saved in the "Snapshot" folder under My Documents in your computer.

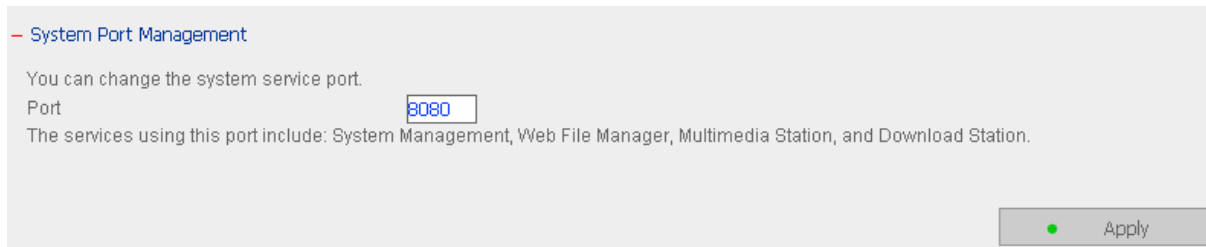


The video recordings will be saved in <\\NASIP\Qrecordings>. Normal recordings are saved in the folder "record\_nvr" and alarm recordings are saved in the folder "record\_nvr\_alarm" in the network share.





### 3.4.14 System Port Management



The screenshot shows a configuration window titled "System Port Management". It contains the following text: "You can change the system service port." followed by a label "Port" and a text input field containing the value "8080". Below the input field, it says "The services using this port include: System Management, Web File Manager, Multimedia Station, and Download Station." In the bottom right corner, there is a button with a green status indicator and the label "Apply".

Assign a protocol for the system management. The default port is 8080. The services of this port include: System Management, Web File Manager, Multimedia Station, and Download Station.

The system will restart after clicking "Apply". Please wait. The website will automatically change to the homepage of the new protocol system.

### 3.4.15 View Network Settings

You can view current network settings and status of the NAS in this section.


[View Network Settings](#)

Network

Network File Services

**LAN Configuration**

Configuration of Network Interfaces	Failover
Network transfer rate	Auto-negotiation
Connection Type	DHCP
IP Address	172.17.28.28
Subnet Mask	255.255.254.0
Default Gateway	172.17.28.1
MAC Address	00:08:9B:BA:9B:4C
Connection Status	100 Mbps, LAN1:Down, LAN2:Up
Enable DHCP Server	No

 Close

- View Network Settings

Network	Network File Services
<b>Microsoft Networking</b>	
Enabled	Yes
Server Type	Standalone Server
Workgroup	NAS
WINS server Enabled	No
Domain Master Enabled	No
<b>Apple Networking</b>	
Enabled	No
Apple Zone Name	*
<b>Unix/Linux NFS</b>	
Enabled	No
<b>Web File Manager</b>	
Enabled	Yes
<b>FTP Service</b>	
Enabled	Yes
Port Number	21
Max Connections	30
<b>Multimedia Station</b>	
Enable Multimedia Station	Yes
Enable iTunes Service	No
Enable UPnP MediaServer	No
<b>Download Station</b>	
Enabled	Yes
<b>Web Server</b>	
Enabled	No
Port Number	80
register_globals	Off
<b>DDNS Service</b>	
Enabled	No
<b>MySQL Server</b>	
Enabled	No
Enable TCP/IP Networking	No
<b>System Port Management</b>	
Port Number	8080

- Close

## 3.5 Device Configuration


You can configure SATA disk, USB disk, eSATA disk, and USB printer settings in this section.

Device Configuration


- SATA Disk
- RAID Management Tool
- Disk Volume Encryption Management
- iSCSI Target
- External Storage Device
- USB Printer

SATA Disk


New Disk Volume Configuration




Single Disk Volume  
Create single disk volume(s).



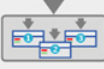
RAID 1 Mirroring Disk Volume  
Create mirroring disk volume(s).




RAID 0 Striping Disk Volume  
Create one striping disk volume.



Linear Disk Volume  
Create one linear disk volume.



RAID 5 Disk Volume  
Combine 3 or more disks to create a disk volume with data protection (1 disk crash is allowed).




RAID 6 Disk Volume  
Combine 4 or more disks to create a disk volume with data protection (2 disk crash is allowed).

Current Disk Volume Configuration

Physical Disks

Disk	Model	Capacity	Status	Bad Blocks Scan	SMART Information
Drive 1	--	--	No Disk	<button>Scan now</button>	---
Drive 2	Seagate ST31000340AS SD15	931.51 GB	Ready	<button>Scan now</button>	Good
Drive 3	Seagate ST3160827AS 3.42	149.05 GB	Ready	<button>Scan now</button>	Good
Drive 4	Seagate ST3500320AS SD15	465.76 GB	Ready	<button>Scan now</button>	Good

Logical Volumes

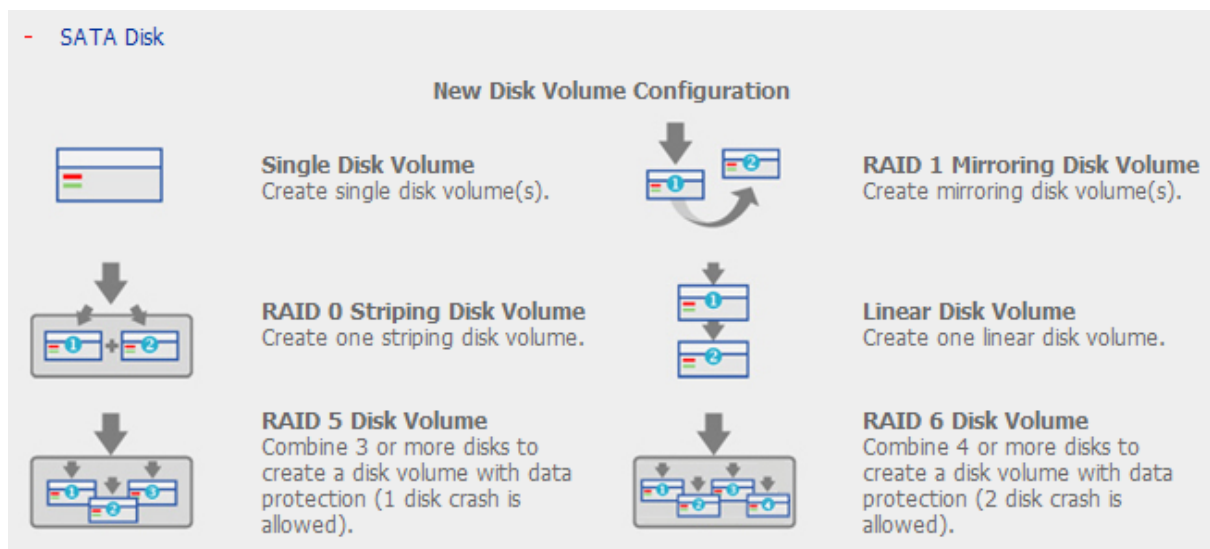
Volume	Total Size	Free Size	Status	Format	Check Disk	Delete Disk Volume
RAID 5 Disk Volume: Drive 2 3 4	290.48 GB	280.22 GB	In degraded mode 	<button>Format now</button>	<button>Check now</button>	<button>Remove now</button>

### 3.5.1 SATA Disk

This page shows the model, size and current status of the disk(s) installed on the NAS. You can format and check disks, and scan bad blocks on the disks. When the SATA disks are formatted, the NAS will create the following default share folders:

- ✓ Public: Network share for file sharing
- ✓ Qdownload: Network share for Download Station
- ✓ Qmultimedia: Network share for Multimedia Station
- ✓ Qusb: Network share for data copy function via USB ports
- ✓ Qweb: Network share for Web Server

You can create the following disk volumes by clicking on the corresponding icon on the "SATA Disk" page.



You can create the following disk volumes:

- **Single Disk Volume**

Each disk is used as a standalone disk. If a disk is damaged, all data will be lost.

- **RAID 1 Mirroring Disk Volume**

RAID 1 (mirroring disk) protects your data by automatically backing up the contents of one drive onto the second drive of a mirrored pair. This protects your data if one of the drives fails. Yet the storing capacity is equal to a single drive, as the second drive is used to automatically back up the first one. RAID 1 is suitable for personal or corporate use to store important data.

- **RAID 0 Striping Disk Volume**

RAID 0 (striping disk) combines 2 or more drives into one larger disk. It offers the fastest disk access but does not have any protection of your data if the striped array fails. The disk capacity equals the number of drives in the array times the size of the smallest drive. Striping disk is usually used to maximize your disk capacity or for fast disk access but not for storing important data.

- **Linear Disk Volume**

You can combine two or more disks into one larger disk. Files are saved on the physical disks sequentially. The overall capacity of linear disk is the sum of all disks. Linear disk is generally used for storing large size of data and is not appropriate for protection of sensitive data.

- **RAID 5 Disk Volume**

RAID 5 disk volume is ideal for organizations running databases and other transaction-based applications that require storage efficiency and data protection. To create a RAID 5 disk volume, a minimum of 3 hard disks are required. The total capacity of RAID 5 disk volume = the size of the smallest capacity disk in the array x (no. of hard disk – 1). It's recommended that you use the same brand and same capacity hard drive to establish the most efficient hard drive capacity.

Additionally, if your system contains four disk drives, three of them can be used to implement RAID 5 data disks and the fourth drive can be used as a spare disk.

When a physical disk failure occurs, the system will automatically rebuild the data with the spare disk.

RAID 5 can survive 1 disk failure and system can still operate properly. When a disk

fails in RAID 5, the disk volume will be in “degraded mode”. There is no more data protection at this stage. If one more disk fails, all the data will be crashed. Therefore, you must replace a new disk immediately. You can install a new disk after turning off the server or hot swap the new disk when the server is on. The status of the disk volume will become “rebuilding” after installing a new disk. When rebuilding completes, your disk volume resumes to normal status.



**Note:** To install a disk when the server is on, make sure the disk volume is in “degraded” mode. Or wait for two long beeps after the disk crash, then insert the new disk.

- **RAID 6 Disk Volume**

RAID 6 disk volume is ideal for important data protection.

To create a RAID 6 disk volume, a minimum of 4 hard disks are required. The total capacity of RAID 6 disk volume = the size of the smallest capacity disk in the array x (no. of hard disk-2). It's recommended that you use same brand and same capacity hard drive to establish the most efficient hard drive capacity.

RAID 6 can survive 2 drives failure and system can still operate properly.



**Note:** To install a disk when the server is on, make sure the disk volume is in “degraded” mode. Or wait for two long beeps after the disk crash, and then insert the new disk.

- **RAID 5, RAID 6 Read-only Mode**

The drive configuration enters read-only mode in the following occasions:

- 2 drives are damaged in RAID 5
- 3 drives are damaged in RAID 6

The drives in the above configurations are read-only. It is recommended to re-create new drive configuration in such case.

## 3.5.2 RAID Management Tool



RAID management tool allows you to carry out capacity expansion, RAID migration, or spare drive configuration with the original drive data reserved.

- RAID Management Tool

This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved.

**Note:** Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Current Disk Volume Configuration

Volume	Total Size	Status	Description
 RAID 5 Disk Volume: Drive 2 3 4	290.48 GB	In degraded mode 	Please insert a drive of larger capacity and wait for the drive status to become Ready before executing this operation.

The operation(s) you can execute:

Expand capacity Add hard drive Migrate Configure spare drive Description

- **Expand capacity**

This function enables drive capacity expansion by replacing the drives in a configuration one by one. This option is supported for the following drive configurations:

- RAID 1 expansion
- RAID 5 expansion
- RAID 6 expansion

- **Add hard drive**

This function enables adding new drive member to a drive configuration. It is supported for the following drive configurations:

- RAID 5 expansion

- **Migrate**

This function enables a drive configuration to be migrated to a different RAID configuration. It is supported for the following drive configurations:

- Migrate single drive to RAID 1, 5, or 6
- Migrate RAID 1 to RAID 5 or 6
- Migrate RAID 5 to RAID 6



- **Configure spare drive**

This function enables adding or removing RAID 5 spare drive. The options available are:

- Add spare drive in RAID 5
- Remove spare drive in RAID 5

For detailed operation, please click the "Description" button on the management interface to view the detailed operation instructions.

### 3.5.3 Disk Volume Encryption Management

You can manage the encrypted disk volumes on the NAS on this page. Each encrypted disk volume is locked by a particular key. The encrypted volume can be unlocked by the following methods:


- Encryption Password: Enter the encryption password to unlock the disk volume. The default password is "admin".
- Encryption Key File: You can upload the encryption file to the server to unlock the disk volume. The key can be downloaded from "Encryption Key Management" page after you have unlocked the disk volume successfully.

#### - Disk Volume Encryption Management

Volume	Total Size	Status	Action
RAID 5 Disk Volume: Drive 2 3 4	290.48 GB	Unlocked	<a href="#">Encryption Key Management</a>

#### Locked Disk Volume

If a disk volume is locked, the disk status is shown as "Unmounted" on "Device Configuration" page and the users are unable to access the disk volume. You can unlock the disk volume by entering the encryption password or uploading the encryption key.

Single Disk: Drive 4	--	--	Unmounted 	<a href="#">Format now</a>	<a href="#">Check now</a>	<a href="#">Remove now</a>
----------------------	----	----	---	----------------------------	---------------------------	----------------------------

If the password entered or uploaded is correct, the disk volume status will be changed to "Unlocked". You can perform further encryption key management on the disk volume.

#### - Disk Volume Encryption Management

Volume	Total Size	Status	Action
Single Disk: Drive 1	145.24 GB	Unlocked	<a href="#">Encryption Key Management</a>

## Encryption Key Management

If the disk volume is shown as “Unlocked”, you can click “Encryption Key Management” to manage the disk volume. On this page, you can change the encryption password, save the encryption key on the system, or download the encryption key to your computer. When you select to save the encryption key, the server will use this key to unlock and mount the disk volume automatically when it is started up.

- Encryption Key Management

Volume: Single Disk Volume: Drive 1

☐ Change Encryption Key

☐ Save Encryption Key

☐ Download Encryption Key File

Ok

Cancel

### 3.5.4 iSCSI Target

The NAS supports built-in iSCSI service. To use this function, follow the steps below:

1. Install an iSCSI initiator on your computer (Windows PC, Mac, or Linux).
2. Enable iSCSI Target Service on the NAS and create a new iSCSI target.
3. Run the iSCSI initiator and connect to the iSCSI target (NAS).
4. After successful logon, format the iSCSI target (disk volume). You can start to use the disk volume on the NAS as a virtual drive on your computer.

**Note:** The NAS supports 8 iSCSI devices at maximum.

- iSCSI Target

☒ Enable iSCSI Target Service

iSCSI Service Port:

☐ Enable iSNS:

iSNS Server IP:

● Apply

- iSCSI Target List

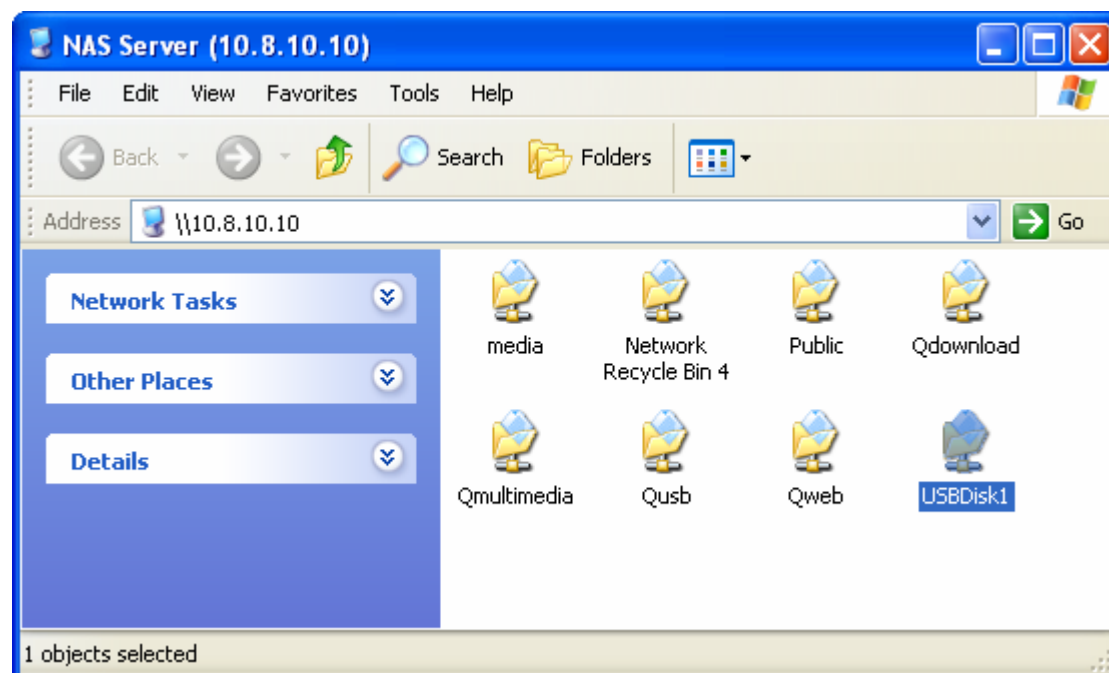
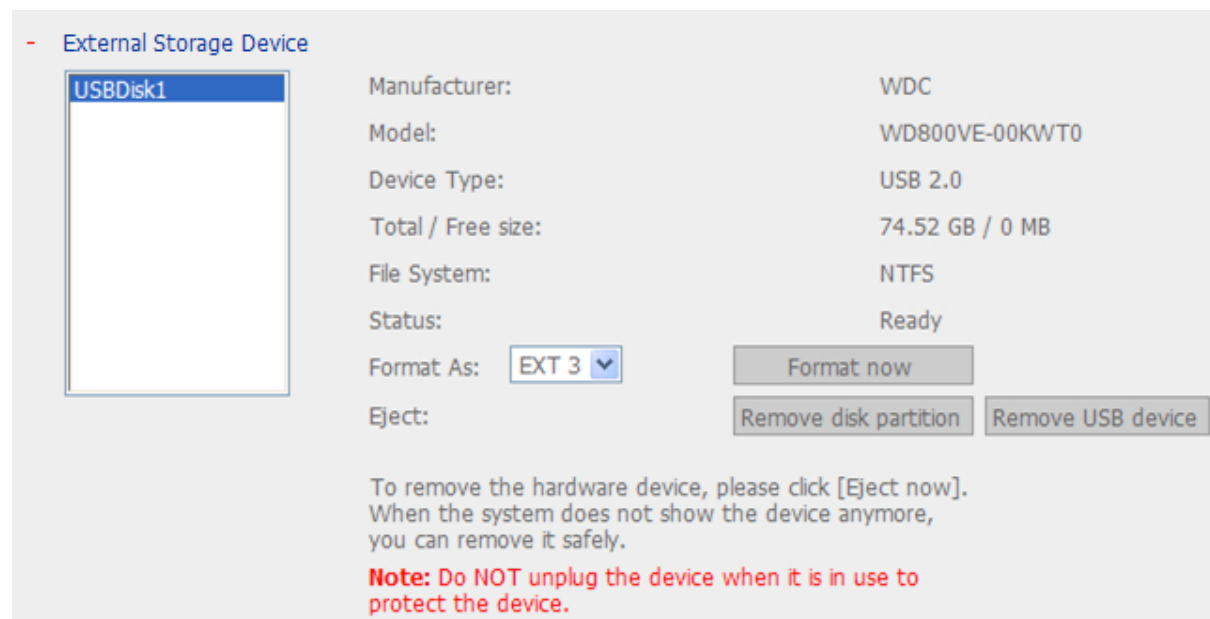
iSCSI Target Name	Capacity	Status	Action
iqn.2004-04.com.qnap:TS-639:iSCSI.test.AB001E	5.00 GB	Ready	<div>Deactivate</div> <div>Modify</div> <div>Delete</div>

Create New iSCSI Target

### 3.5.5 External Storage Device

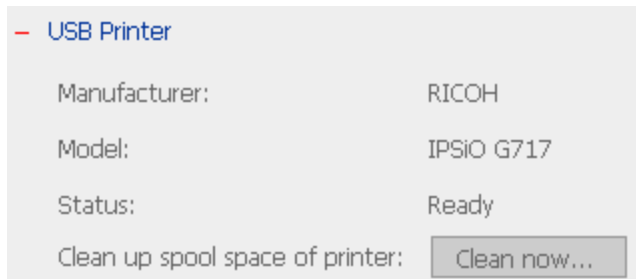
The NAS supports eSATA disks, USB disks, and thumb drives for extended storage. Connect the eSATA device to the eSATA port, or connect the USB device to a USB port of the NAS. When the device is successfully detected, the details are shown on this page.

It may take tens of seconds for the NAS server to detect the external storage device successfully. Please wait patiently.



### 3.5.6 USB Printer

To provide printer sharing function for network users, you can simply connect a USB printer to the USB port of the NAS. The NAS will detect the printer automatically. This function supports up to 3 printers.

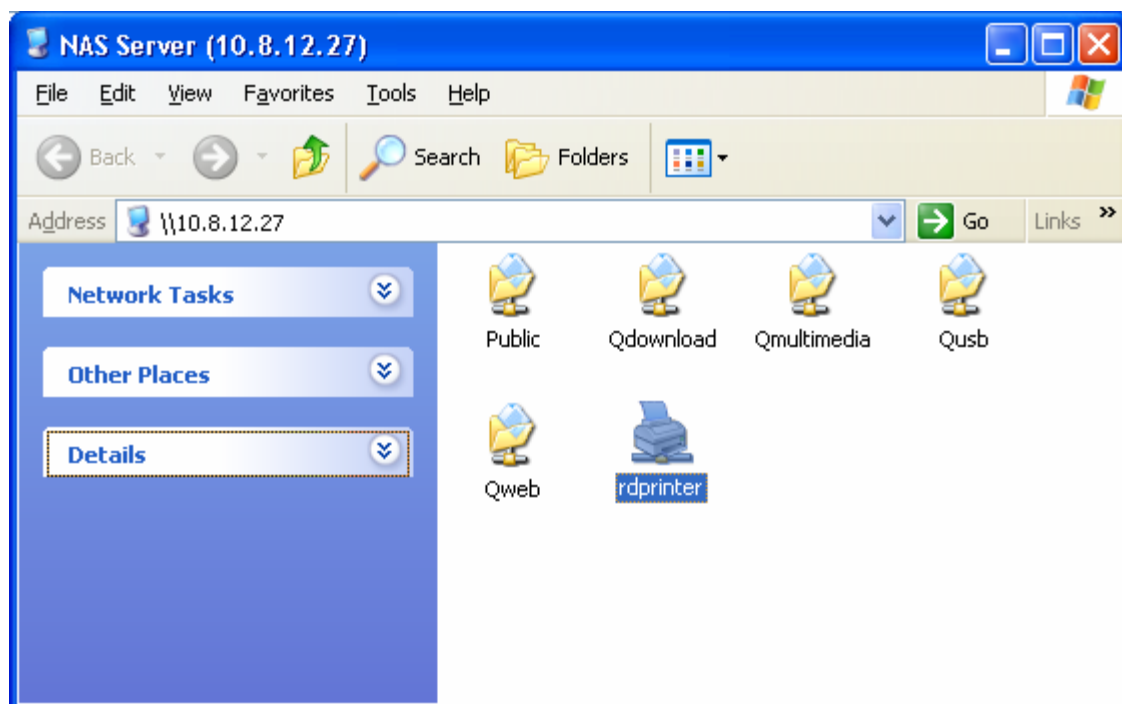


**Note:** Please connect a USB printer to the server after the software configuration is completed.

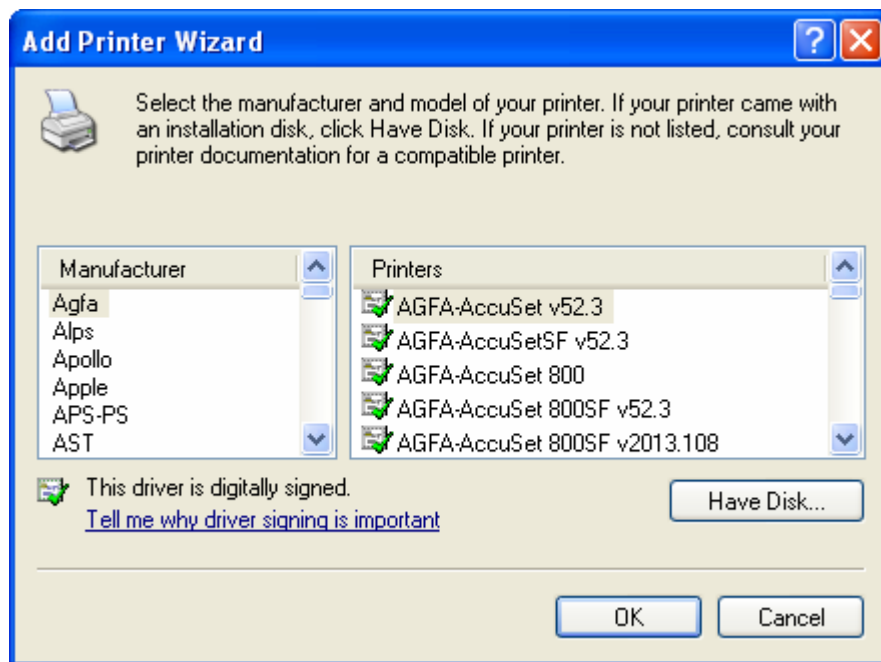
#### 3.5.6.1 Windows Users

##### Method 1

1. A printer icon should be shown in the share folder of the server. Double click the icon.



2. Install the printer driver.



3. When finished, you can start to use network printer service of the NAS.

## Method 2

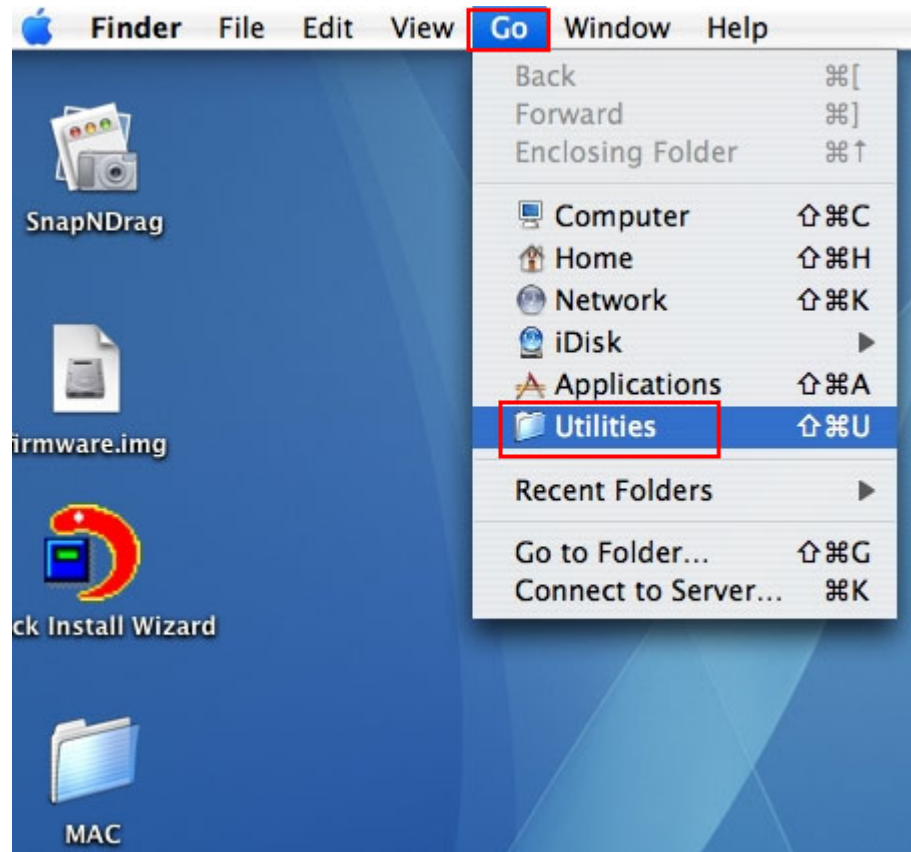
The following configuration method has been verified on Windows XP only:

5. Open "Printers and Faxes".
6. Delete the existing network printer (if any).
7. Right click the blank area in the Printers and Faxes window. Select "Server Properties".
8. Click the Ports tab and delete the ports configured for the previous network printer (if any).
9. Restart your PC.
10. Open Printers and Faxes.
11. Click "Add a printer" and click "Next".
12. Select "Local printer attached to this computer". Click "Next".
13. Click "Create a new port" and select "Local Port" from the drop-down menu. Click "Next".
14. Enter the port name. The format is \\NAS IP\NAS namepr, e.g. NAS IP= 192.168.1.1, NAS name= myNAS, the link is \\192.168.1.1\myNAS**pr**.
15. Install the printer driver.
16. Print a test page.

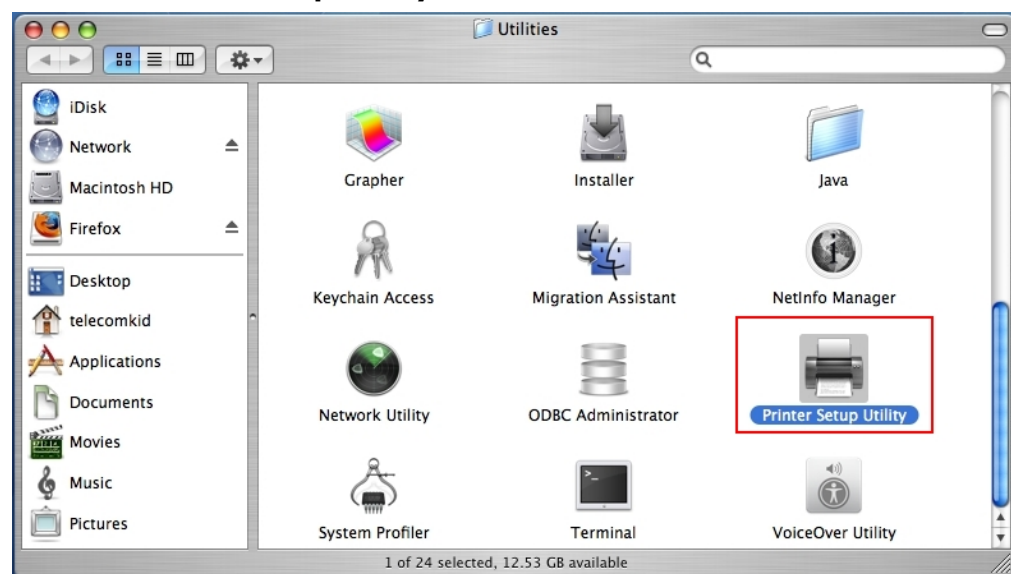


### 3.5.6.2 Mac Users

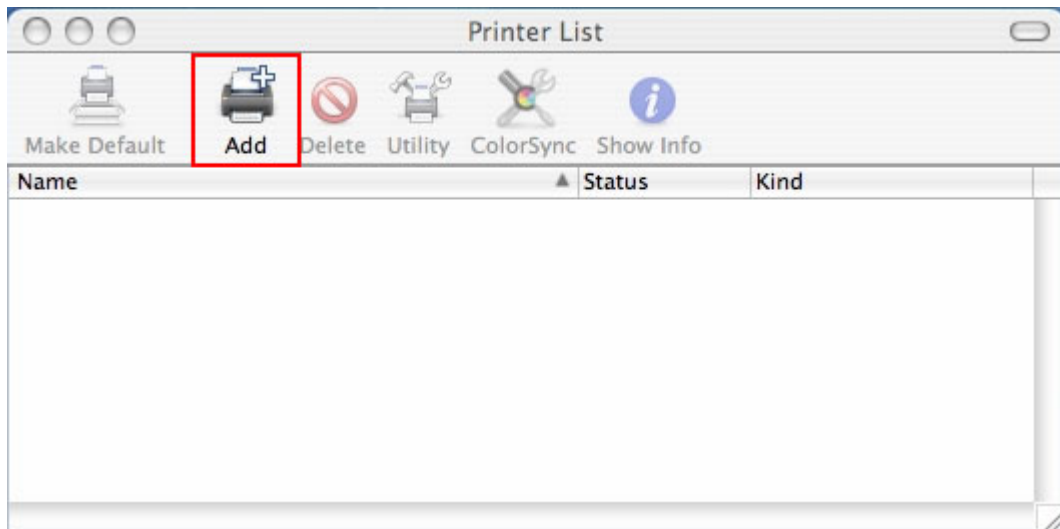
1. On the toolbar, click **Go/ Utilities**.




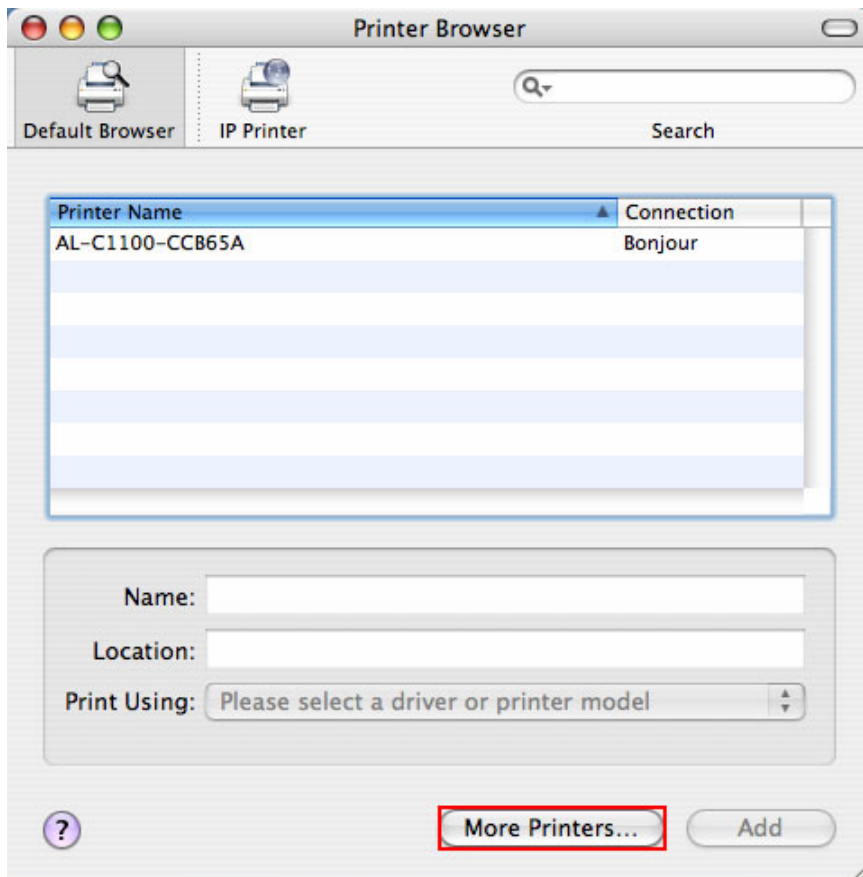
2. Click **Printer Setup Utility**.



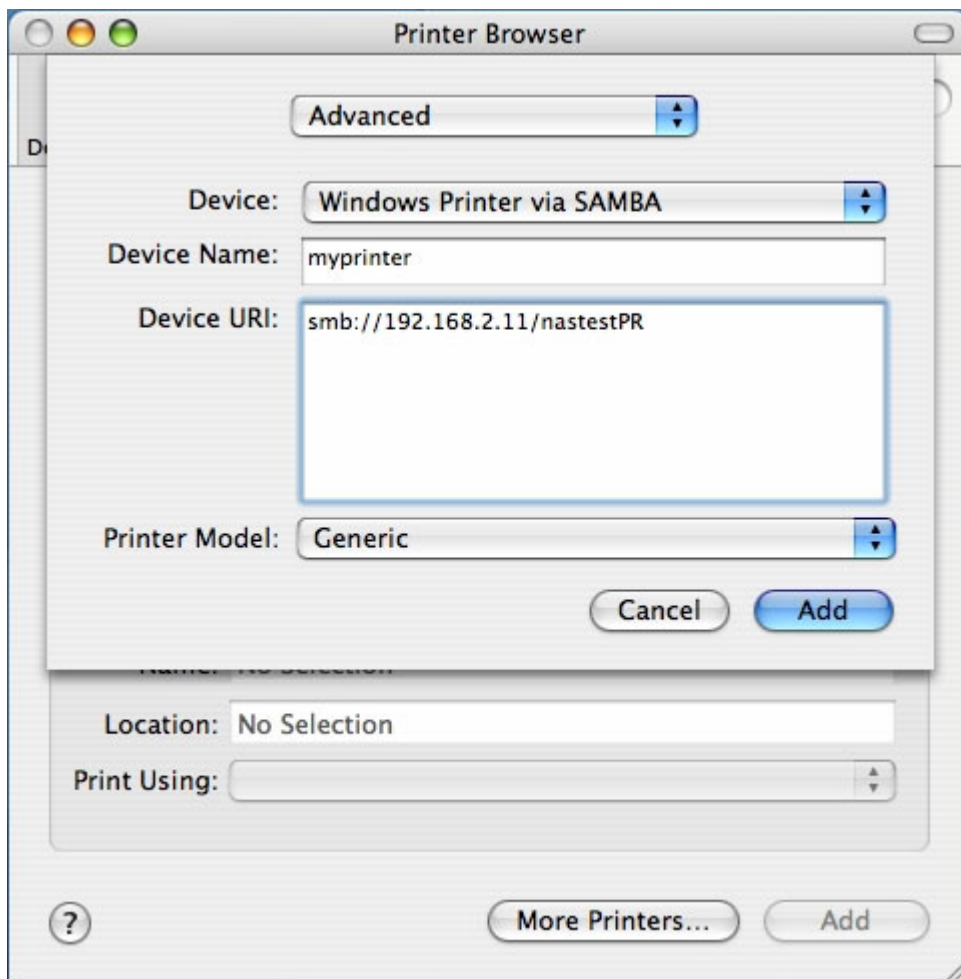
3. Click **Add**.



4. Press and hold the **alt** key  on the keyboard and click **More Printers** concurrently.

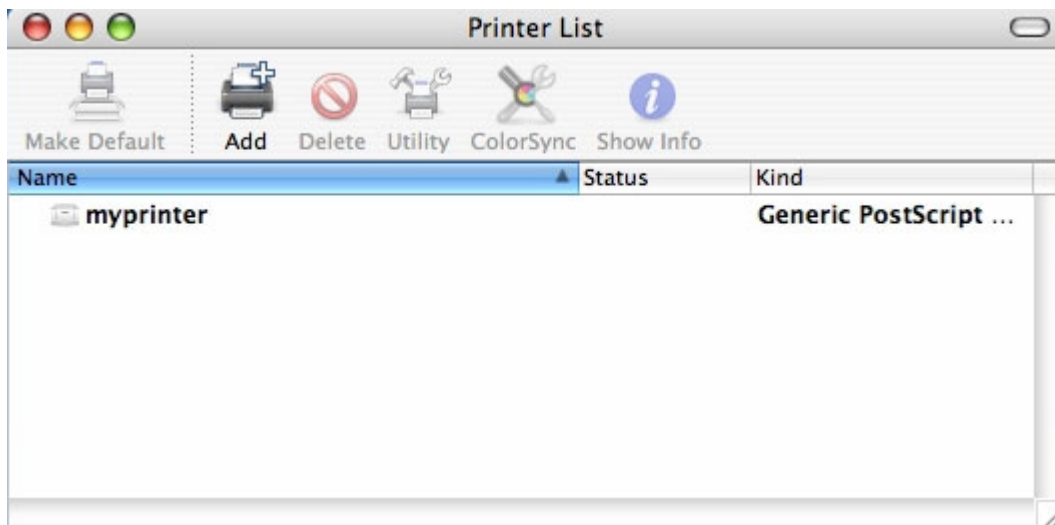


5. In the pop up window:
  - a. Select **Advanced**\*
  - b. Select **Windows Printer with SAMBA**.
  - c. Enter the printer name.
  - d. Enter the printer URI, the format is smb://NAS IP/printer name. The printer name is found on the Device Configuration/ USB Printer page.
  - e. Select **Generic** for Printer Model.
  - f. Click **Add**.



\*Note that you must hold and press the **alt** key and click **More Printers** at the same time to view the Advanced printer settings. Otherwise, this option does not appear.

6. The printer appears on the printer list. It is ready to use.

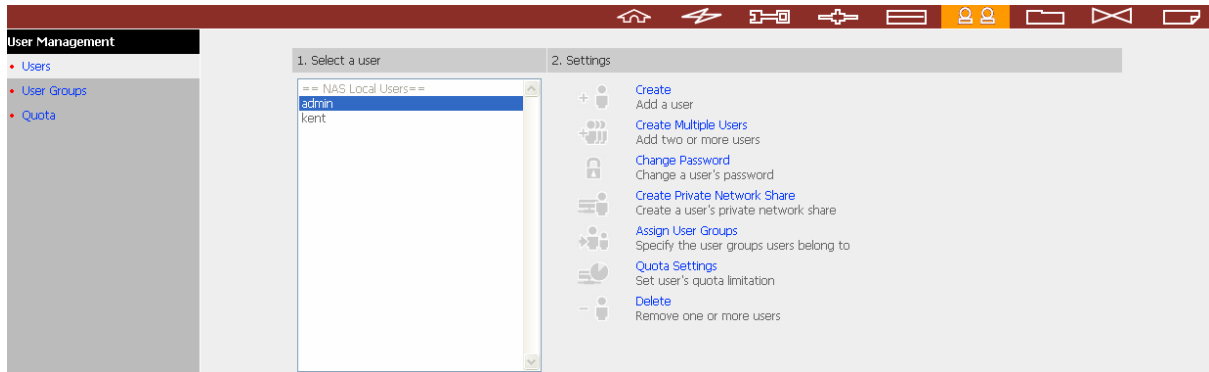


**Note:**

1. The NAS network printer service supports Postscript printer on Mac OS only.
2. For the latest USB printer compatibility list, please visit <http://www.qnap.com>.

## 3.6 User Management

The files on the NAS can be shared among multiple users. For easier management and better control of users' access right, you have to organize users, user groups and their access right control.



### 3.6.1 Users

The system has created the following users by default:

- **admin**  
By default, admin has access to system administration and cannot be deleted.
- **guest**  
This is a built-in user and will not be displayed on User Management page. A guest does not belong to any user group. The login password for guest is **guest**.
- **Anonymous**  
This is a built-in user and will not be displayed on User Management page. When you connect to the server by FTP service, you can use this name to login as a guest.

**512 users can be created at maximum** (including system default users). You can create a new user according to your needs. The following information is required to create a new user:

✓ **User name**

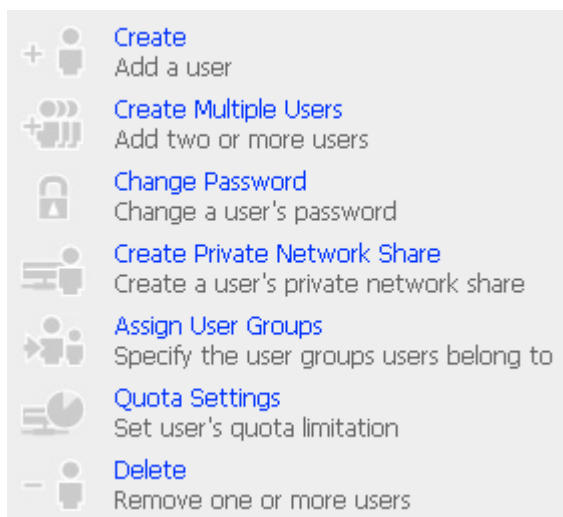
The user name must not exceed 32 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean excluding:

" / \ [ ] : ; | = , + \* ? < > ` '

✓ **Password**

The password is case-sensitive and can be 16 characters long at maximum. It is recommended to use a password of at least 6 characters.

You can perform the following actions for user management:



### 3.6.1.1 Create user

To create a user, click "Create" and enter the user name and password.

The screenshot shows a dialog box titled "Add a user". It contains three input fields: "User Name" with the text "user01", "Password" with "\*\*\*\*\*", and "Verify Password" with "\*\*\*\*\*". Below these fields is a note: "Note: For increased security, password should be at least 6 characters." At the bottom left, there is a checked checkbox labeled "Continue to set the user groups to which this user belongs". At the bottom right, there are two buttons: "OK" and "Cancel".

You can continue to assign the user groups that the user belongs to. Click "Close" to exit.

The screenshot shows a dialog box titled "Specify the user groups users belong to". It has two list boxes. The left list box is titled "User groups which user01 belongs to" and contains the text "everyone". The right list box is titled "User groups which user01 doesn't belong to" and contains the text "administrators" and "beta". Between the two list boxes are two buttons: "Add" with a green arrow pointing left and "Remove" with a red arrow pointing right. At the bottom right, there is a "Close" button.

### 3.6.1.2 Create Multiple Users

The NAS enables you to create multiple users at one time. Click "Create Multiple Users". Enter the name prefix, e.g. test. Enter the start number for the user name, e.g. 0001 and the number of users to be created, e.g. 10. The NAS creates ten users named test0001, test0002, test0003...test0010. The password entered here is the same for all new users. You can change the password in the "User Management" > "Users" page.

— Add two or more users

User Name Prefix	<input type="text" value="test"/>
User Name Start No.	<input type="text" value="0001"/>
User Number	<input type="text" value="0010"/>
Password	<input type="password" value="*****"/>
Verify Password	<input type="password" value="*****"/>

☒ Create Private Network Share

Hide network drive ☐ Yes ☒ No (Hide this network drive in My Network Places. However, the drive can still be shown by entering the directory manually in My Network Places.)

Disk Volume

**Note:** For increased security, password should be at least 6 characters.

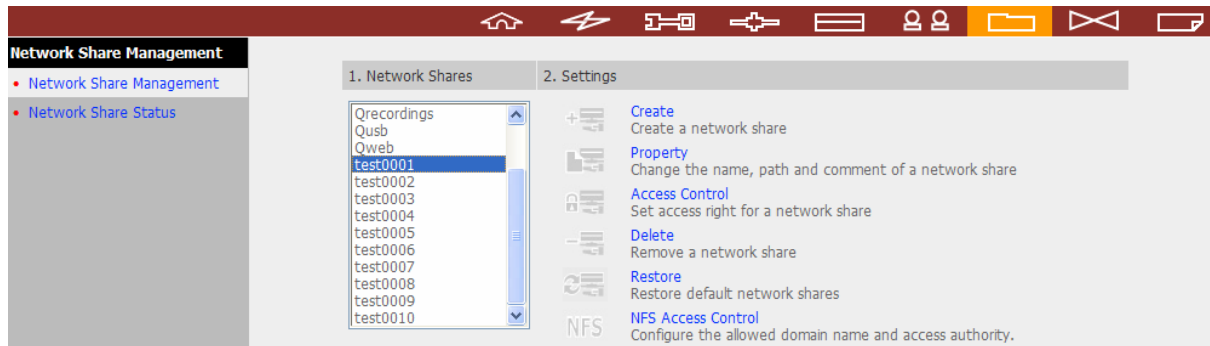
OK Cancel

1. Select a user	2. Settings
<div><div>QATEST+user93</div><div>QATEST+user94</div><div>QATEST+user95</div><div>QATEST+user96</div><div>QATEST+user97</div><div>QATEST+user98</div><div>QATEST+user99</div><div>== NAS Local Users ==</div><div>admin</div><div>kent</div><div>test0001</div><div>test0002</div><div>test0003</div><div>test0004</div><div>test0005</div><div>test0006</div><div>test0007</div><div>test0008</div><div>test0009</div><div>test0010</div></div>	<div><div>+ </div><div>Create</div><div>Add a user</div></div> <div><div>+ </div><div>Create Multiple Users</div><div>Add two or more users</div></div> <div><div></div><div>Change Password</div><div>Change a user's password</div></div> <div><div>+ </div><div>Create Private Network Share</div><div>Create a user's private network share</div></div> <div><div>+ </div><div>Assign User Groups</div><div>Specify the user groups users belong to</div></div> <div><div>+ </div><div>Quota Settings</div><div>Set user's quota limitation</div></div> <div><div>- </div><div>Delete</div><div>Remove one or more users</div></div>





**Note:** When you check the option “Create Private Network Share” for creating multiple users, a network share named in the user name is created for each newly created user.



### 3.6.2 User Groups

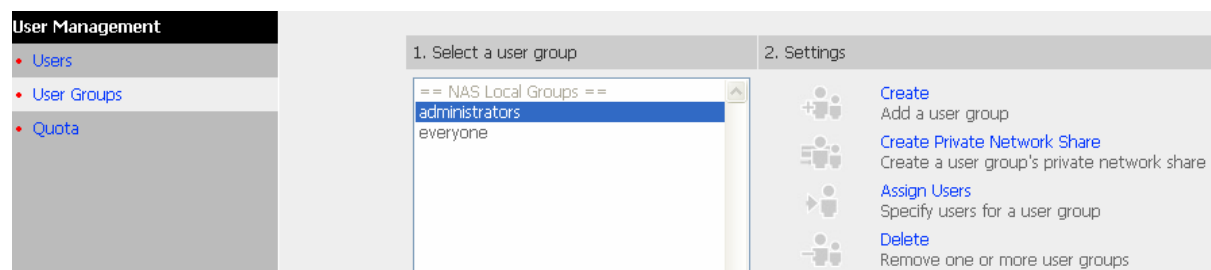
User group is a collection of users with the same access right to files or folders. The NAS has created the following user groups by default:

- **Administrators**

All members in this group have administration right. You cannot delete this group.

- **Everyone**

All registered users belong to everyone group. You cannot delete this group.



You can manage user groups with the following options:



**1024 groups can be created at maximum.** A group name must not exceed 256 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean, except the following ones:

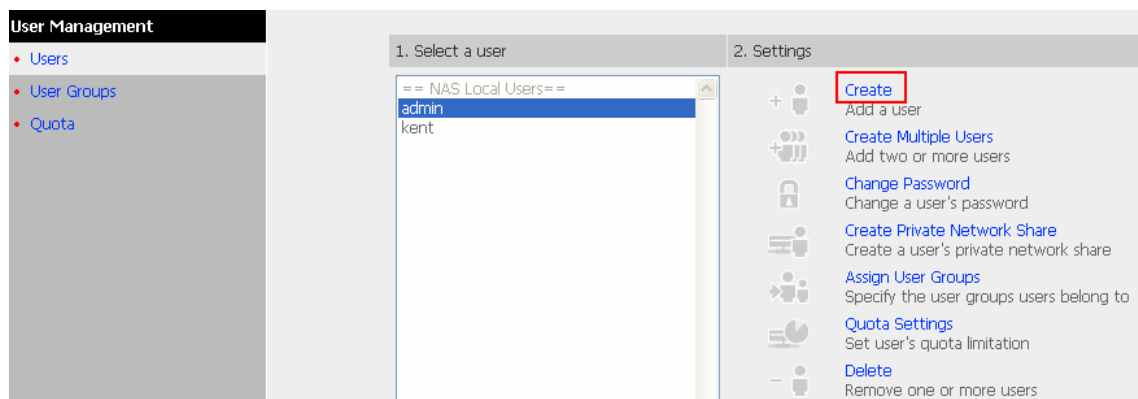
" / \ [ ] : ; | = , + \* ? < > ` '

## Create Users and Assign Users to User Group

The following example demonstrates how to create new users and assign users to a user group.

ABC Co. has recently recruited two employees Jones Lee for Administration Department and Jane Wu for Sales Department. The IT Department therefore needs to create two user accounts for them to access company data on the NAS.

- i. To create a user account, go to User Management-Users. Click **Create**.



- ii. Enter the user name (Jones Lee/ Jane Wu) and password. Check the box “Continue to set the user groups to which this user belongs” and click **OK**.

– Add a user

User Name

Password

Verify Password

**Note:** For increased security, password should be at least 6 characters.

☒ Continue to set the user groups to which this user belongs

– Add a user

User Name

Password

Verify Password

**Note:** For increased security, password should be at least 6 characters.

☒ Continue to set the user groups to which this user belongs

- iii. Select the user groups the users belong to on the right list, i.e. Jones Lee for Administration Dept and Jane Wu for Sales Dept, and click **Add**. Then click **Close**.

– Specify the user groups users belong to

User groups which **Jones Lee** belongs to

everyone

User groups which **Jones Lee** doesn't belong to

Administration Dept  
Sales Dept  
administrators

← Add

Remove →

Close

– Specify the user groups users belong to

User groups which **Jane Wu** belongs to

everyone

User groups which **Jane Wu** doesn't belong to

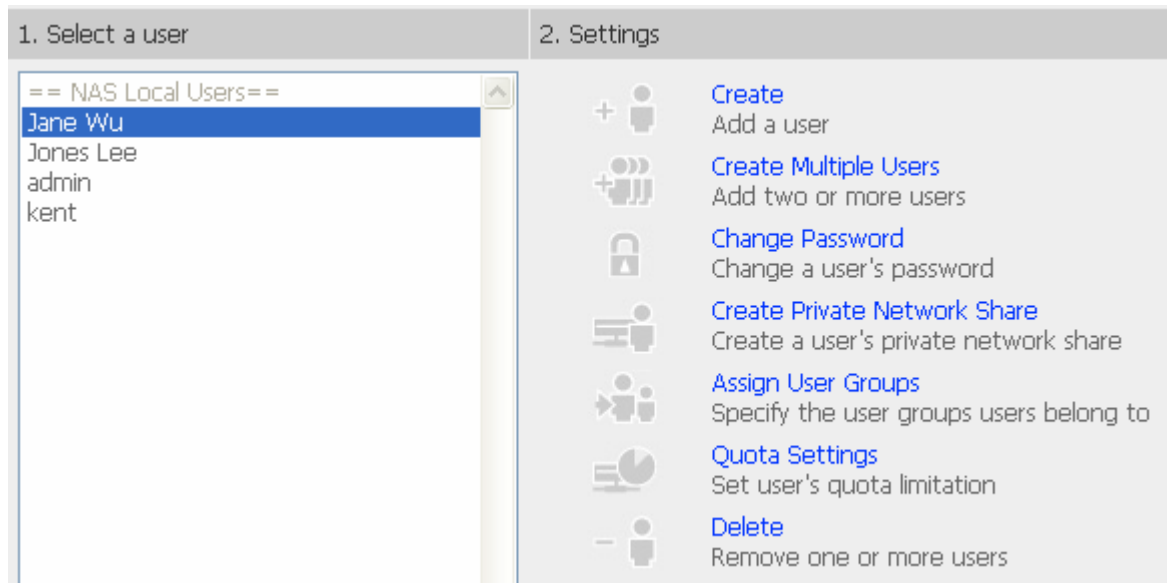
Administration Dept  
Sales Dept  
administrators

← Add

Remove →

Close

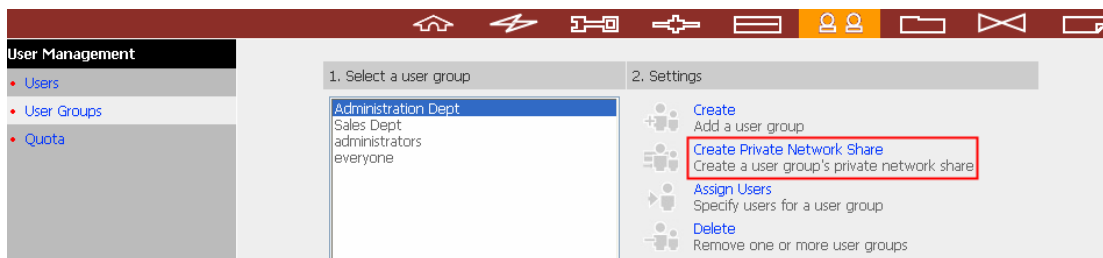
iv. The user names will appear on the list on Create User page.



## Create Private Network Share for User Groups

You can create particular network share for each user group. The procedure is described as below:

1. To create a network share called "media" accessible by the Administration Department only, go to "User Management-User Groups" page. Select the user group Administration Dept and click "Create Private Network Share" on the right.



2. Enter the network share name "media". Select the disk volume that the share will be created in and specify the path automatically or manually. Enter the comment for the network share, e.g. media folder for Admin Dept and click "Apply".

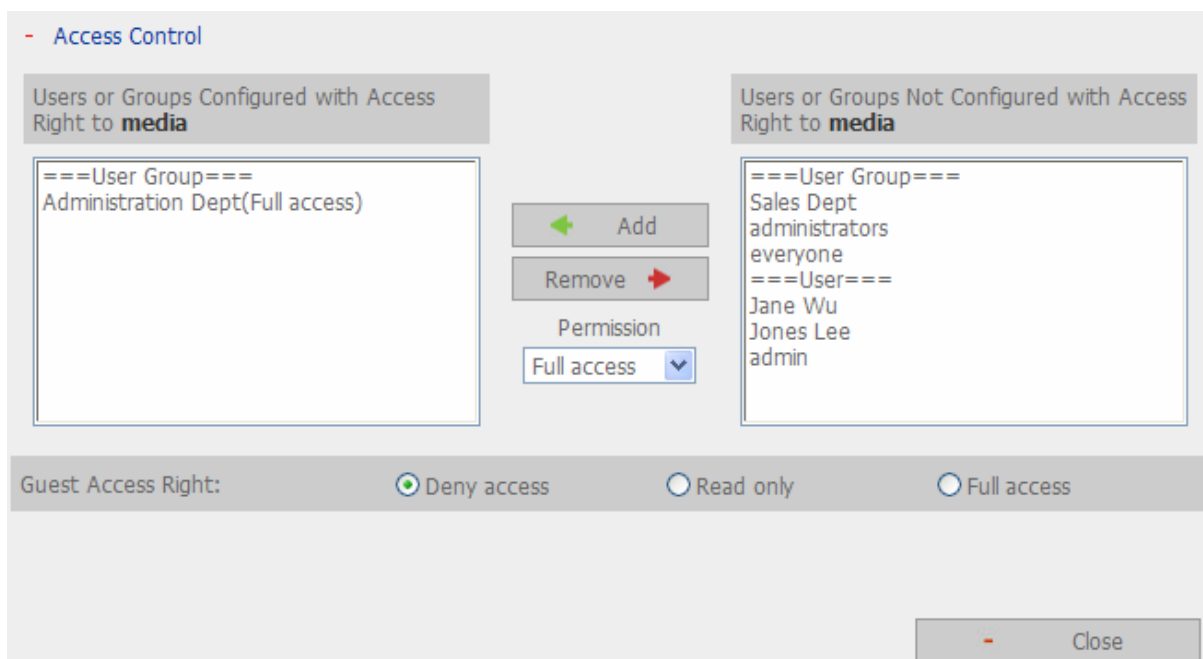
- Enter new network share's name, volume and path. Only users that are the members of Administration Dept user group can access this network share.

Network Share Name	<input type="text" value="media"/>
Hide network drive	<input type="radio"/> Yes <input checked="" type="radio"/> No (Hide this network drive in My Network Places. However, the drive can still be shown by entering the directory manually in My Network Places.)
Lock file (oplocks)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Disk Volume	<input type="text" value="Single Disk: Drive1"/>
Path	<input checked="" type="radio"/> Specify path automatically <input type="radio"/> Enter path manually
Comment	<input type="text" value="media folder for Admin Dept"/>

3. You can see the folder "media" on the "Network Share Management" page.



4. Enter Access Control. You can see that only Administration Dept has full access right to the folder.

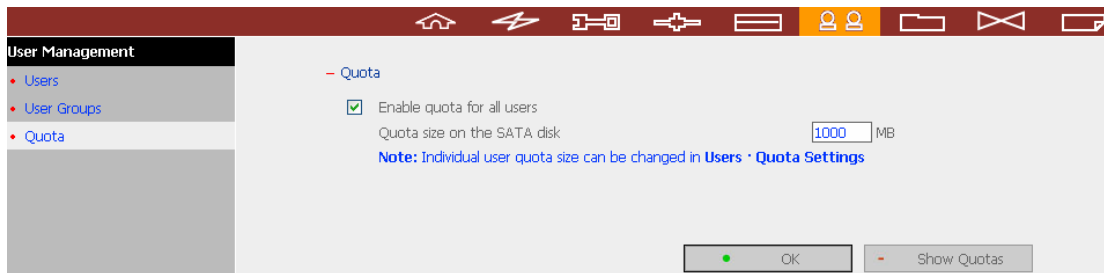




### 3.6.3 Quota

To allocate disk volume efficiently, specify the quota that can be used by each user. When you have reached the disk quota, you cannot upload data to the server anymore. By default, no limitations are set for users. You can modify the following two options:

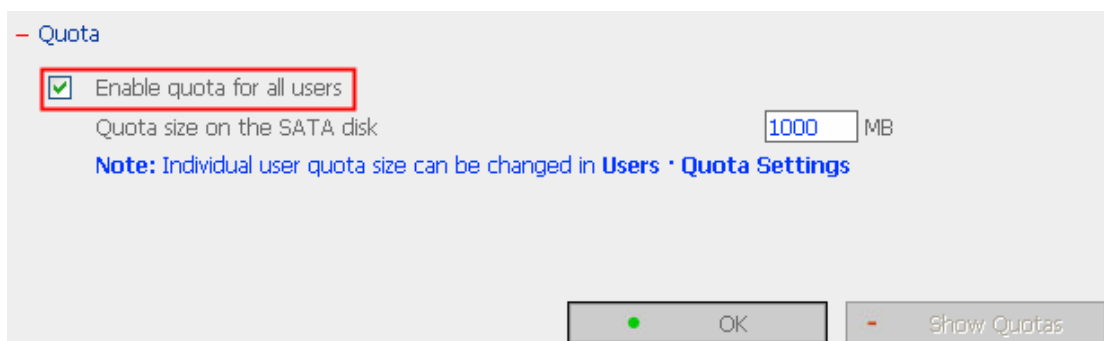
- i. Enable quota for all users
- ii. Quota size on each disk volume



Please refer to the following example to configure the quota setting of users:

The IT department is planning to set the disk quota of Jones Lee from Administration Department and Jane Wu from Sales Department on the NAS. The disk quota is 2000MB for Jones Lee and 4000MB for Jane Wu.

1. Please go to "Quota" page in "User Management" to enable quota for all users. Enter the quota size on each disk volume, e.g. 1000MB. The quota for an individual user can be modified later.



2. Select Jones Lee on User page and click "Quota Settings" on the right.

The screenshot shows the 'User Management' interface. On the left, there is a sidebar with 'Users', 'User Groups', and 'Quota'. The main area is divided into two panels: '1. Select a user' and '2. Settings'. In the '1. Select a user' panel, a list of users is shown: '== NAS Local Users==', 'Jane Wu', 'Jones Lee' (highlighted), and 'admin'. In the '2. Settings' panel, several options are listed: 'Create', 'Create Multiple Users', 'Change Password', 'Create Private Network Share', 'Assign User Groups', 'Quota Settings' (highlighted with a red box), and 'Delete'.

3. Enter the quota size 2000MB and click "OK".

The screenshot shows a dialog box titled 'Quota status for user Jones Lee'. It contains a table with the following data:

Volume	Quota Size	Used Size	Status
Single Disk: Drive (Free Size: 149190.00 MB)	1000 MB	0.00 MB	Available 1000.00 MB

Below the table, there is a section titled 'Set the quota size of Jones Lee on the SATA disk'. It contains two radio buttons: 'No limit' and 'Quota size: 2000 MB'. The 'Quota size' option is selected. At the bottom, there are 'OK' and 'Cancel' buttons.

4. Follow the same steps and enter the quota size 4000MB for Jane Wu and click "OK".  
The quota setting is successfully applied.

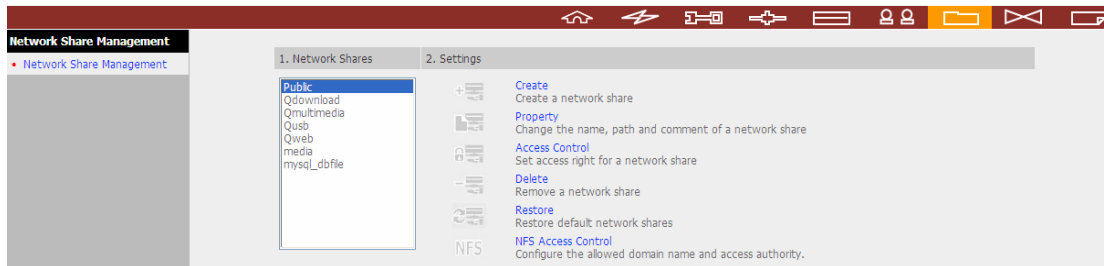
The screenshot shows a dialog box titled 'Quota status for user Jane Wu'. It contains a table with the following data:

Volume	Quota Size	Used Size	Status
Single Disk: Drive (Free Size: 149190.00 MB)	1000 MB	0.00 MB	Available 1000.00 MB

Below the table, there is a section titled 'Set the quota size of Jane Wu on the SATA disk'. It contains two radio buttons: 'No limit' and 'Quota size: 4000 MB'. The 'Quota size' option is selected. At the bottom, there are 'OK' and 'Cancel' buttons.

## 3.7 Network Share Management

The primary purpose of network storage is file sharing. You can create different network share folders for various types of files, and provide different file access rights to users or user groups.



### 3.7.1 Network Share Management

#### 3.7.1.1 Create

To create a network share, enter the following information:

✓ Network share name

The length of the network share name cannot exceed 32 single-byte characters or 10 double-byte characters, and cannot contain the following characters:

**" . + = / \ : | \* ? < > ; [ ] %**

✓ Hide network drive

Select to show or hide the network in My Network Places. Note that the drive can still be shown by entering the directory manually in My Network Places.

✓ Lock file (oplocks)

When "Yes" is selected, the oplock value of the network share in smb.conf is yes. If a user with write access opens a file in the network share by Microsoft network (samba) connection and another user opens the file in the same way, the file will become read-only to the latter user.

When "No" is selected, the oplock value of the network share in smb.conf is no. Any users with write access can edit and save the files in the network share by Microsoft network (samba) connection.

✓ Disk volume

This area shows the disk volume status.

✓ Path

All data is stored under the assigned path onto the disk volume. You can select "Specify path automatically" or assign a path manually. The path cannot exceed 256 characters and cannot contain the characters below:

" . + = / \ : | \* ? < > ; [ ] %

✓ Comment

Enter a brief description for the share folder. The comment cannot exceed 128 characters.

- Create

Network Share Name

Hide network drive ☐ Yes ☒ No (Hide this network drive in My Network Places. However, the drive can still be shown by entering the directory manually in My Network Places.)

Lock file (oplocks) ☒ Yes ☐ No

Disk Volume

Path ☒ Specify path automatically ☐ Enter path manually

Comment

☒ Grant full access right for everyone

☐ Grant read access right for guest

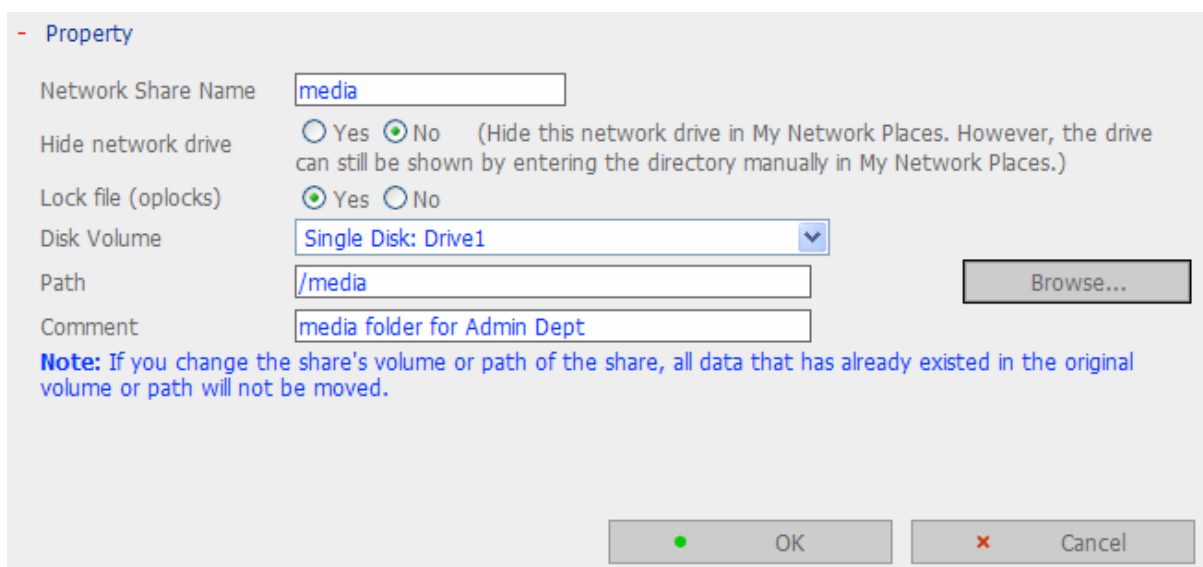
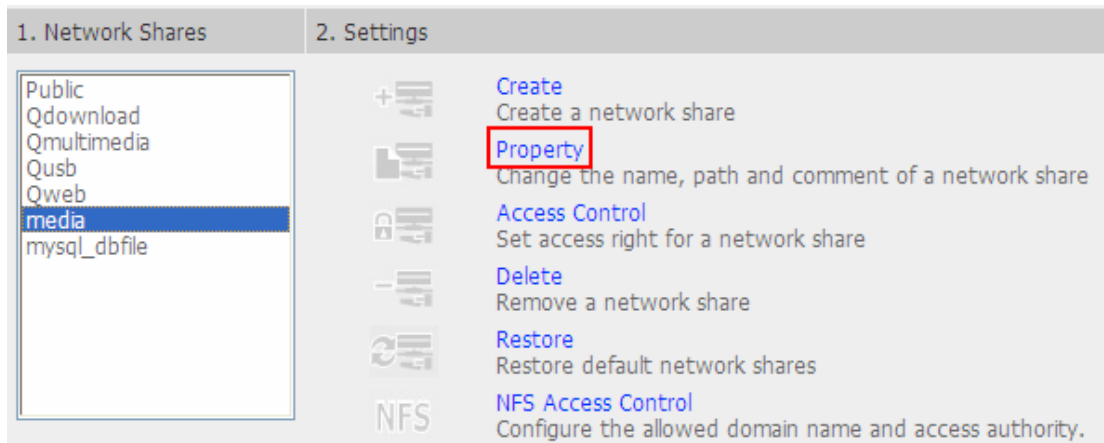
☒ Continue to set access right for this network share



**Note:** When you select to enter the path manually, click "Browse..." and the .@mysql directory will be shown. This is the file location of MySQL database.

### 3.7.1.2 Property

To edit the property of an existing network share, select a share and click **Property**. You can then edit the content of that share.



### 3.7.1.3 Access Control

When a network share is created, you can assign access rights to users or user groups:

- ✓ Deny access  
Access to the network share will be denied.
- ✓ Read only  
Users can read the files only on the network share.
- ✓ Full access  
Users can read, write, create, or delete files and folders on the network share.
- ✓ Enable write-only access on FTP connection  
When you enable this option, only the administrator "admin" has read and write access to the share folder. Other users who have full access to the share folder will only be able to upload files to the folder via FTP connection but are unable to see the folder contents.

The screenshot shows the 'Access Control' dialog box for a network share named 'media'. The dialog is divided into two main sections: 'Users or Groups Configured with Access Right to media' and 'Users or Groups Not Configured with Access Right to media'. In the first section, a list box contains 'Admin Dept(Full access)'. In the second section, a list box contains 'administrators', 'everyone', and 'admin'. Between these sections are buttons for 'Add' (with a left arrow), 'Remove' (with a right arrow), and a 'Permission' dropdown menu currently set to 'Full access'. Below these sections, there are three radio buttons for 'Guest Access Right': 'Deny access' (selected), 'Read only', and 'Full access'. At the bottom, there is a checkbox labeled 'Enable write-only access on FTP connection' which is checked. Below this checkbox is a descriptive text: 'When this option is enabled, only "admin" has read and write access to the network share. All other users with full access to the share folder originally will only be able to write the folder.' A 'Close' button is located in the bottom right corner.

- Access Control

Users or Groups Configured with Access Right to **media**

===User Group===  
Admin Dept(Full access)

Users or Groups Not Configured with Access Right to **media**

===User Group===  
administrators  
everyone  
===User===  
admin

← Add

Remove →

Permission  
Full access ▼

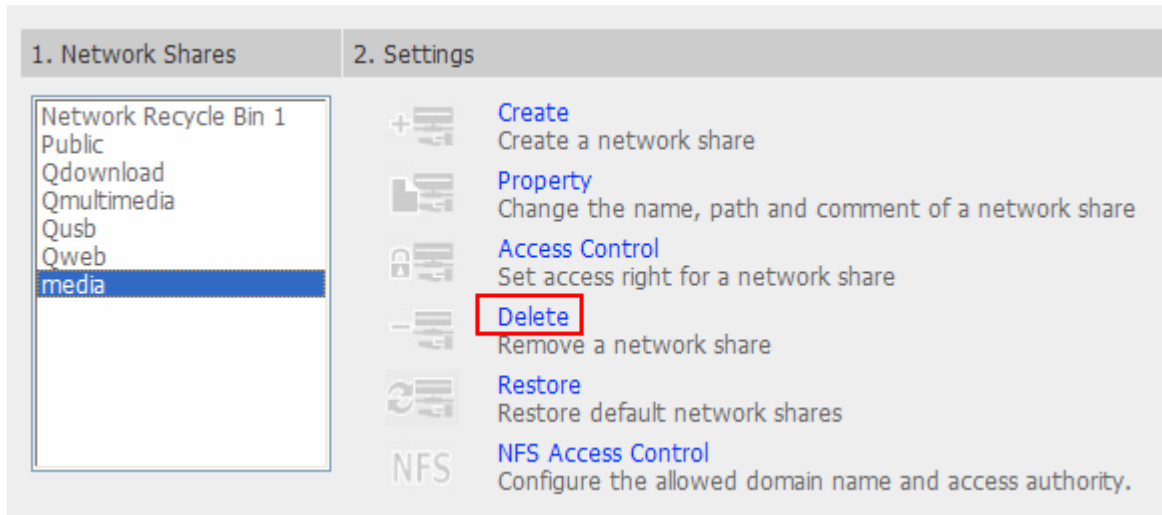
Guest Access Right: ☒ Deny access ☐ Read only ☐ Full access

☒ Enable write-only access on FTP connection  
When this option is enabled, only "admin" has read and write access to the network share. All other users with full access to the share folder originally will only be able to write the folder.

Close

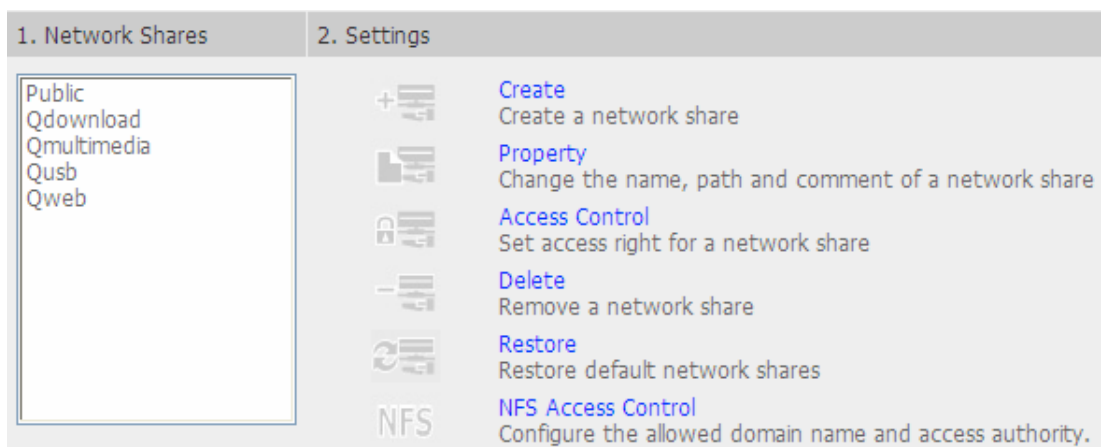
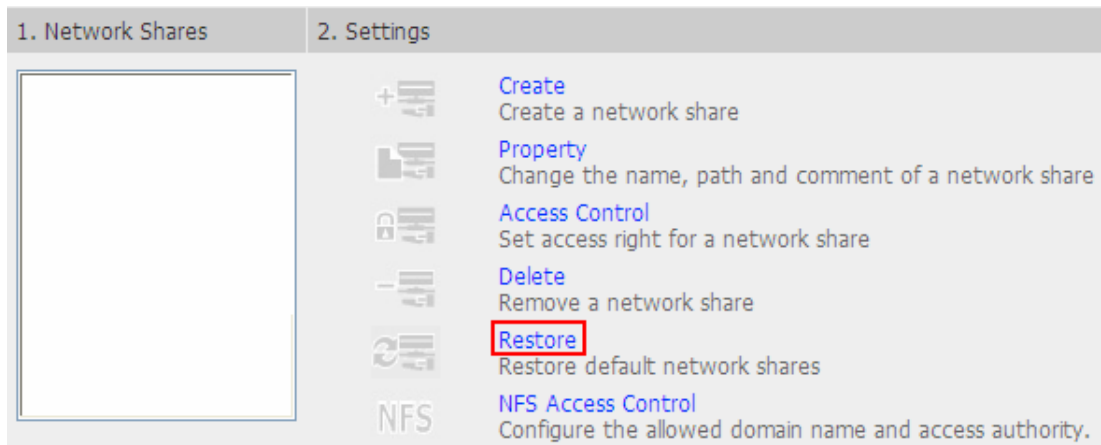
#### 3.7.1.4 Delete

Select a share and click "Delete". Click "OK" to confirm.



### 3.7.1.5 Restore

If the default network shares of the NAS are not created successfully, you can use the Restore function to restore the network shares. To do so, click **Restore** and the shares will be created.





### 3.7.1.6 NFS Access Control

You can set the NFS access right of the network share. The Public folder is for open access while the access is denied for other default network shares by default.

- NFS Access Control

You can set the NFS access right of the network share.

Network Share Name: Public

Access right: No limit

Allowed IP address or domain name: \*







Note: Please make sure the format you enter is correct. An incorrect format can lead to access error.

The allowed IP address or domain name can be a complete IP address or a domain name searchable by DNS. The IP addresses and domain names can be separated by comma (,). Wildcard characters "\*" and "?" are supported for domain names, e.g. \*.yourdomain.com. For further details. [Click here for more detailed description.](#)

OK Cancel

### 3.7.2 Network Share Status

This page shows the status of the network share folders of the system including the storage capacity, number of folders and files etc. You can click on "Name", "Size", "No. of Folders", "No. of Files", or "Hidden" to sort the contents in ascending or descending order. To refresh the status report of a network share folder, click the icon at the end of row. The time for updating the information depends on the number of folders and files in the network share folder.

- Network Share Status						
Name	Size	No. of Folders	No. of Files	Hidden	Comment	
Network Recycle Bin 1	4.03 KB	0	1	No	[Single Disk Volume: Drive 1]	
Public	4 KB	0	0	No	System default share	
Qdownload	4 KB	0	0	No	System default share	
Qmultimedia	8 KB	3	0	No	System default share	
Qusb	4 KB	0	0	No	System default share	
Qweb	4 KB	0	0	No	System default share	

## 3.8 System Tools

The System Tools enable you to optimize the maintenance and management of the NAS.

The screenshot displays the 'System Tools' web interface. On the left is a sidebar menu with various system management options. The main content area is titled 'Alert Notification' and contains settings for email and SMS alerts. The 'Alert Notification' section explains that alerts are sent automatically when a system event occurs. It includes dropdown menus for 'Send system error alert by:' and 'Send system warning alert by:', both currently set to 'No alert'. Below these are the '[Email Notification Settings]' which include two empty text boxes for 'E-mail address 1:' and 'E-mail address 2:', and a checkbox for 'Send a test e-mail'. A note states that the SMTP server must be configured first. The '[SMS Notification Settings]' section includes a dropdown for 'Country Code:' set to 'Afghanistan (+93)', and two empty text boxes for 'Cell Phone No. 1:' and 'Cell Phone No. 2:', both with a '+93' prefix. A note explains that the SMSC server must be configured properly. At the bottom right is an 'Apply' button.

**System Tools**

- Alert Notification
- Auto Power on/off Management
- Hardware Settings
- UPS
- Hard Disk SMART
- System Update
- USB one touch copy backup
- Change Logo
- Back up to an external storage device
- Remote Replication
- Backup/ Restore/ Reset Settings
- IP Filter
- Network Recycle Bin
- Remote Login
- QPKG
- Import SSL Secure Certificate

**Alert Notification**

When a system event occurs, an alert email will be sent automatically.

Send system error alert by:

Send system warning alert by:

[Email Notification Settings]

E-mail address 1:

E-mail address 2:

☐ Send a test e-mail

Note: The SMTP server must be configured first for alert mail delivery. [Click this to configure the SMTP server](#)

[SMS Notification Settings]

Country Code:

Cell Phone No. 1: +93  (Do not enter the beginning "0".)

Cell Phone No. 2: +93  (Do not enter the beginning "0".)

☐ Send a test SMS message (If the SMSC settings are incorrect, you will not be able to receive the test message.)

Note: You must configure the SMSC server to be able to send SMS notification properly. [Click here to configure the SMSC server.](#)

### 3.8.1 Alert Notification

You can configure to receive instant SMS or email alert when a system error or warning occurs. Enter the email address and mobile phone number to receive the alerts. Make sure you have entered the correct SMTP server and the SMSC server settings. If you do not want to receive any alerts, select "No alert" for both settings.

**Alert Notification**

When a system event occurs, an alert email will be sent automatically.

Send system error alert by: No alert

Send system warning alert by: No alert

**[Email Notification Settings]**

E-mail address 1:

E-mail address 2:

☐ Send a test e-mail

Note: The SMTP server must be configured first for alert mail delivery.[Click this to configure the SMTP server](#)

**[SMS Notification Settings]**

Country Code: Afghanistan (+93)

Cell Phone No. 1: +93  (Do not enter the beginning "0".)

Cell Phone No. 2: +93  (Do not enter the beginning "0".)

☐ Send a test SMS message (If the SMSC settings are incorrect, you will not be able to receive the test message.)

Note: You must configure the SMSC server to be able to send SMS notification properly. [Click here to configure the SMSC server.](#)

● Apply

### 3.8.2 Auto Power on/ off Management

This section enables you to restart or shut down the server immediately, set schedule for automatic system power on/ off/ restart, and enable "Wake on LAN". You can also configure the option the server should do when the AC power resumes after an abnormal power failure, e.g. the power cord is unplugged.

You can select every day, weekdays, weekend, or any days of the week and set the time for automatic system power on, power off, or restart. Weekdays stand for Monday to Friday; weekend stands for Saturday and Sunday. Up to 15 schedules can be set.

- Auto Power on/off Management

Execute system restart/ shutdown immediately

Restart

Shut Down

Configure Wake on LAN

☐ Enable ☒ Disable

When the AC power resumes:

☒ Resume the server to the previous power-on or power-off status.

☐ Turn on the server automatically.

☐ The server should remain off.

Set power on/ power off/ restart schedule

☐ Enable schedule

Shut Down

Daily

7

0

+

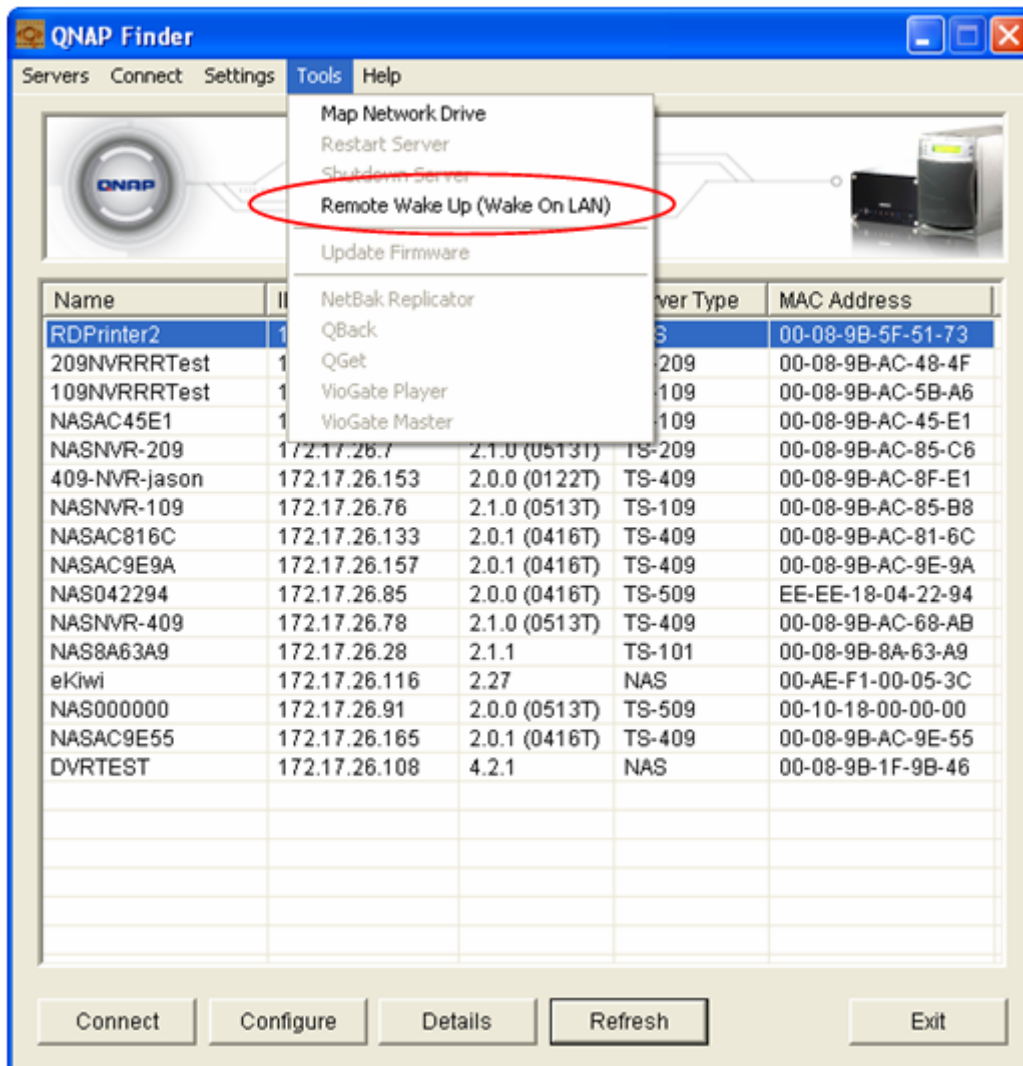
-

Apply

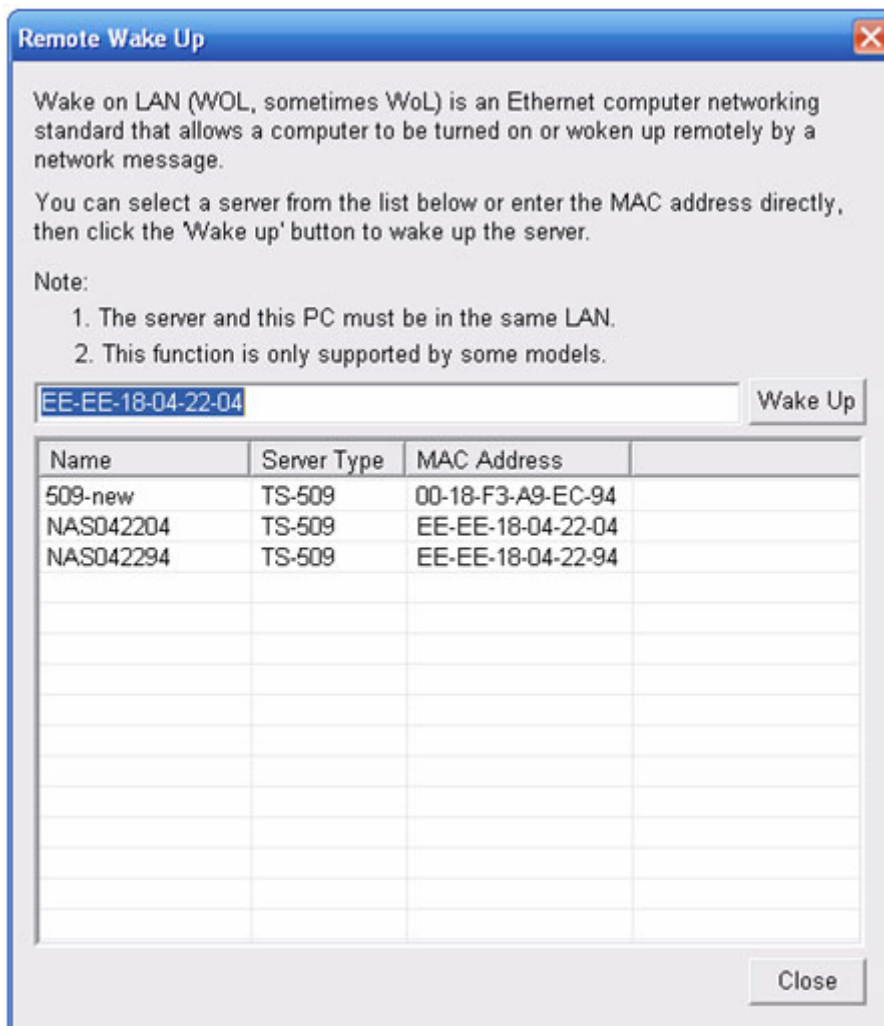
## Wake on LAN

The Wake on LAN option enables you to power on the NAS remotely. To use this function, follow the steps below. Make sure this option is enabled in "System Tools>Auto Power on/off management" page on the NAS.

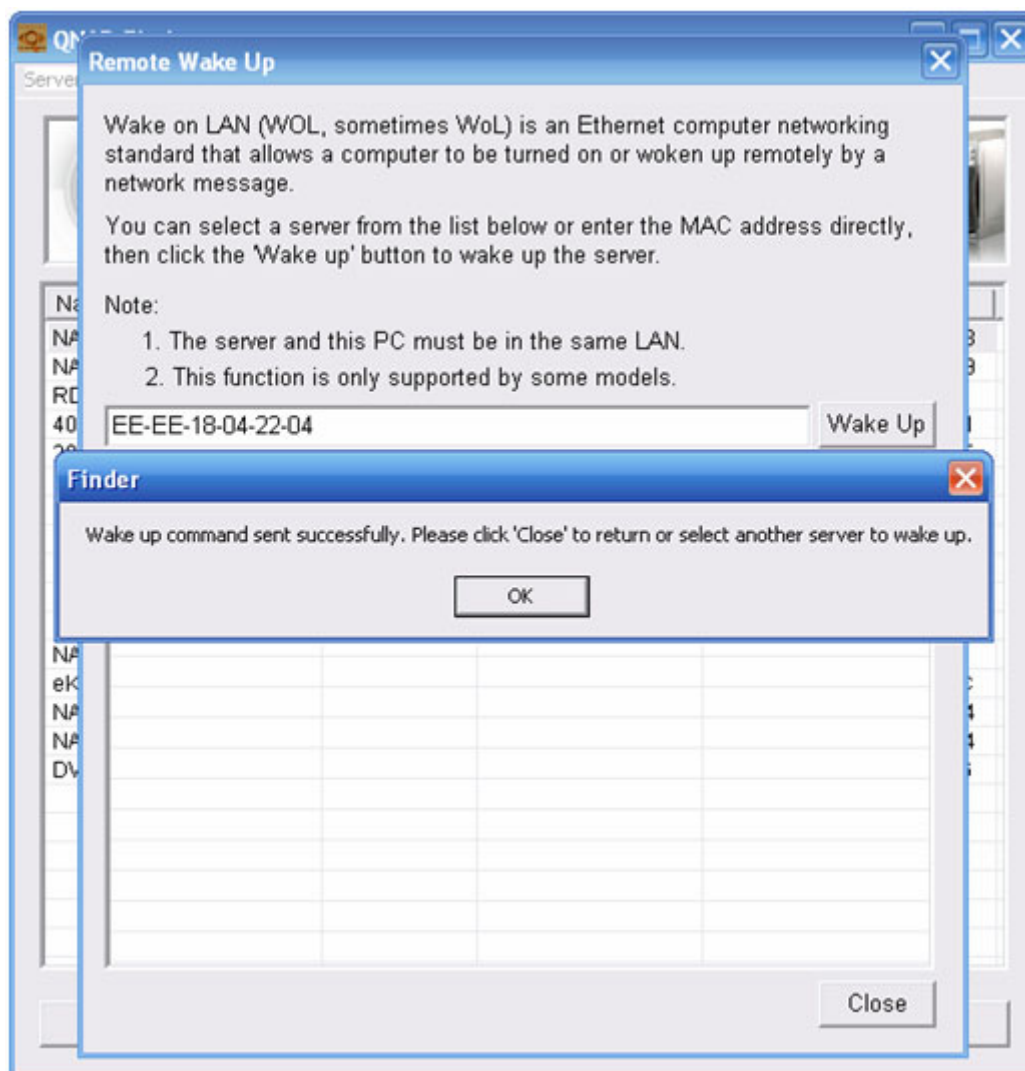
1. Run QNAP Finder. Click "Tools" on the menu and select "Remote Wake Up (Wake On LAN)".



2. A list of supported NAS models detected in the LAN will be shown. Select the server you want to wake up or enter the MAC address of the NAS server and click "Wake up".



3. After sending the command, click "Close" to exit. Refresh the Finder to search for the server. If the NAS is found, it has been turned on successfully.





### 3.8.3 Hardware Settings

You can enable or disable the hardware functions of the NAS.

- Hardware Settings

- ☒ Enable configuration reset switch
- ☒ Enable hard disk standby mode (if no access within  Status LED will be off)
- ☒ Enable light signal alert when the free size of SATA disk is less than the value:  MB
- ☐ Enable alarm buzzer (beep sound for error and warning alert)

Fan rotation speed settings:

☒ When the system temperature is lower than 47°C, rotate at low speed. When the system temperature is higher than 52°C, rotate at high speed.

☐ Self-defined temperature:

When the system temperature is lower than  °C stop fan rotation.

When the system temperature is lower than  °C, rotate at low speed.

When the system temperature is higher than:  °C, rotate at high speed.

- i. Enable configuration reset switch  
By enabling this option, you can press the reset button for 3 seconds to reset the administrator password and system settings to default.
- ii. Enable hard disk standby mode  
When this function is enabled, hard disk will go to standby mode if there is no access within the specified period. The Status LED will be off.
- iii. Enable light signal alert when the free size of SATA disk is less than the value  
The Status LED flashes red and green when this function is enabled and the free space of the SATA disk is less than the value. The range of the value is 1-51200 MB.
- iv. Enable alarm buzzer  
Enable this option. The system will sound when an error occurs.
- v. Smart Fan configuration  
After enabling Smart Fan, the fan rotation speed is automatically adjusted according to the server temperature. It is recommended to enable this option. By manually setting the fan rotation speed, the fan rotates at the defined speed continuously.

### 3.8.4 UPS

You can enable UPS (uninterruptible power supply) support to protect your system from abnormal system shutdown caused by power outage.

- UPS

☒ Enable UPS Support

☒ After the AC power fails for 5 minute(s), turn off the server.

☐ After the AC power fails for 2 minute(s), the server should enter standby mode. When the power resumes, the system resumes to the operation status.

UPS Model: USB UPS (auto detect) ▼

IP Address of UPS: 0 . 0 . 0 . 0

---

UPS Information

UPS Brand: --

UPS Model: --

AC Power Status: --

Battery Capacity: --

Estimated Protection Time: --

Refresh Apply

✓ **Enable UPS support**

To activate the UPS support, you can select this option. You can set the shutdown timer to turn off the system automatically after the system detects the AC power is abnormal. In general, the UPS can keep supplying the power for the system for about 5~10 minutes, depending on the maximum load of the UPS and the number of the loads connected to it. You may also configure the system to enter standby mode in case of abnormal AC power supply.

✓ **UPS Model**

Select the UPS model from the list. If the UPS model you are using is not available on the list, please contact our technical support.

✓ **IP Address of UPS**

If you have selected APC UPS with SNMP for UPS model, enter the IP address of the UPS.

### 3.8.5 Hard Disk S.M.A.R.T.

This page enables users to monitor hard drive health, temperature, and usage status by the hard disk S.M.A.R.T. mechanism.

Select the hard drive and you can view the following information by clicking the corresponding buttons.

Field	Description
Summary	Displays the hard drive smart summary and the latest test result.
Hard disk information	Displays the hard drive details, e.g., model, serial number, drive capacity, etc.
SMART information	Displays the hard drive SMART. Any items that the values are lower than the threshold are regarded as abnormal.
Test	To perform quick or complete hard drive SMART test and display the results.
Settings	To configure temperature alarm. When the hard drive temperature is over the preset values, the system records error logs. You can also configure quick and complete test schedule. The latest test result is shown in the Summary page.

— Monitor hard disk health, temperature, and usage status by the hard disk S.M.A.R.T. mechanism.

Select hard disk: Disk 1 ▾

Summary

Hard Disk Information

SMART Information

Test

Settings

Good

No errors were detected on the hard disk. Your hard disk should be operating properly.

---

Hard disk model	Seagate Barracuda 7200.10 family
Drive capacity	232.89 GB
Hard drive health	Good
Hard drive temperature	47 °C ▾
Test time	---
Test result	Not tested

### 3.8.6 System Update

- System Update

**Note:** If the system is running properly, you do not need to update the firmware.

Current firmware version: 2.1.0 Build 1215T

Before updating system firmware, please make sure the product model and firmware version are correct. Follow the steps below to update firmware:

Step 1: Download the release notes of the same version as the firmware from QNAP website <http://www.qnap.com/> Read the release notes carefully to make sure you need to update the firmware.

Step 2: Before updating system firmware, back up all disk data on the server to avoid any potential data loss during system update.

Step 3: Click the **[Browse...]** button to select the correct firmware image for system update. Click the **[Update System]** button to update the firmware.

**Note:** System update may take tens of seconds to several minutes to complete depending on the network connection status. Please wait patiently. The system will inform you when system update is completed.

Update System



**Note:** If the system is running properly, you do not need to update the firmware.

Before updating system firmware, please make sure the product model and firmware version are correct. Follow the steps below to update firmware:

**Step 1:** Download the release notes of the same version as the firmware from QNAP website <http://www.qnap.com/>. Read the release notes carefully to make sure you need to upgrade the firmware.

**Step 2:** Before upgrading system firmware, back up all disk data on the server to avoid any potential data loss during system update.

**Step 3:** Click "Browse..." to select the correct firmware image for system update. Click "Update System" to update the firmware.



**Note:** System update may take tens of seconds to several minutes to complete depending on the network connection status. Please wait patiently. The system will inform you when system update is completed.

### 3.8.7 USB One Touch Copy Backup

You can configure the function of the USB one touch copy button in this page. The following three functions are available:

- Copy from the front USB storage to a directory of the internal drive of the NAS.
- Copy to the front USB storage from a directory of the internal drive of the NAS.
- Disable the one touch copy button

- USB one touch copy backup

To configure the function of the USB one touch copy button.

☒ Copy from the front USB storage device to the 

Qusb

 directory of the internal disk.  
Backup method: 

Add directory

 Back up data to the newly created directory on the destination sharing folder

☐ Copy to the front USB storage device from the 

Qusb

 directory of the internal disk.

☐ Disable one touch copy button

Note: The USB LED blinks when data backup to an external device is in process. The USB one touch copy button will be disabled temporarily. If you press the button during the data transfer process, the server will beep thrice to alert you the button is disabled. Please wait for the backup to finish and the USB LED to stop flashing, and then use the USB one touch copy button again.

Apply

### 3.8.8 Change Logo

You can choose your own picture to display on the login page of the NAS. The size of the picture cannot exceed 20K bytes.

#### Change Logo

Please select an image from the **To be displayed** pull-down menu. Then click **[Apply]** to confirm the change.

To upload your own image, click **[Browse...]** to select the image. Then click **[Upload]** to upload the image.

To replace an image, select an appropriate image from the **To be replaced to** pull-down menu and click **[Apply]**.

Uploaded image:

Browse...

Upload

To be replaced to:

Not replace

▼

Replace

To be displayed:

Image 1

▼

Image 1

Image 2

Uploaded Image

Image 3

Image 4

Current Logo Image

---

**Note:** For the best image effect, the recommended size for the image is 100 x 100 pixels.

●

Apply

### 3.8.9 Back up to an External Storage Device

– Back up to an external storage device

Back up the local disk data to an external storage device. You can select instant, automatic, or schedule backup.

The network drives for backup

The network drives not for backup

Create

Delete

USB Disk 1

No external device is detected currently.

Free Size/Total Size: --

Backup method :

Backup Now

Execute backup immediately.

Copy options :

Copy

Back up data to the destination drive.

Current backup status :

No backup operations.

Last backup time :

---

Last backup result :

---

OK

You can back up the local drive data to an external storage device. In this page, you can select to execute instant, automatic, or schedule backup methods, and configure the relevant settings.

- Backup Now: To back up data to the external storage device immediately.
- Schedule Backup: To back up data by schedule. You can select the week day and time to execute the backup.
- Auto-backup: To execute the backup automatically once the storage device is connected to the NAS.

#### Copy Options:

Select "Copy" or "Synchronize" for the copy options. When you select "Copy", files are copied from the NAS to the external device. By selecting "Synchronize", the data on the internal drives of the NAS and the external storage device are synchronized. Any different files on the external device are deleted.



**Note:** In the copying and synchronizing process, if the identical files exist on both sides, the files are not copied. If there are files in the same name but different in size or modified dates on NAS and the external device, the files on the external device are overwritten.



### 3.8.10 Remote Replication (Disaster Recovery)

You can use this option to back up the files on the NAS to another QNAP NAS or Rsync server over LAN or the Internet.

**Make sure a network share is created before creating a remote replication task.**

#### Using Remote Replication

Login the NAS and go to "Remote Replication" in "System Tools".

- ✓ **Port Number:** Specify a port number for remote replication. The default port number is 873.



**Note:** If this server connects to the Internet via a router, make sure the specified port for remote replication is opened on the router.

- ✓ **Enable backup from a remote server to the local host:** Check this option to allow the remote server to back up data to the local host via remote replication.
- ✓ **Allow remote Rsync server to back up data to NAS:** Enable this option to allow a remote server to back up data to the NAS by remote replication.

Remote Replication

By using this function, you can back up the data on the local server to a remote server of the same NAS series, and also allow backup from remote server to the local server.

Port Number:

☒ Enable backup from a remote server to the local host.

☐ Allow remote Rsync server to back up data to NAS

OK

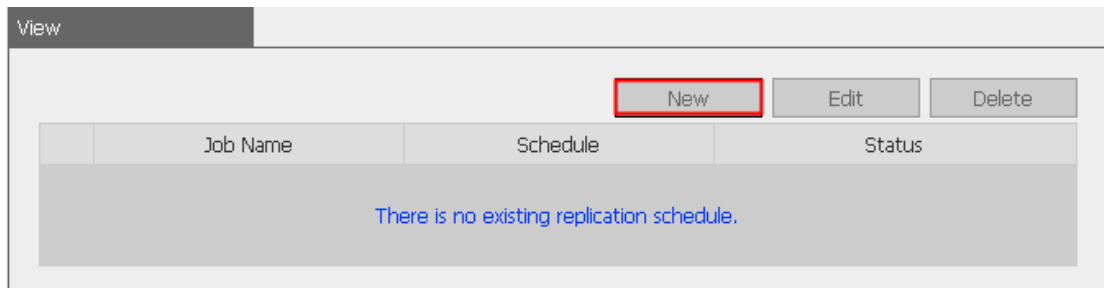
View

NewEditDelete

	Job Name	Schedule	Status
There is no existing replication schedule.			

Follow the steps below to create a remote replication job for backup from the NAS to another QNAP NAS.

- a. Click "New" to create a new task.

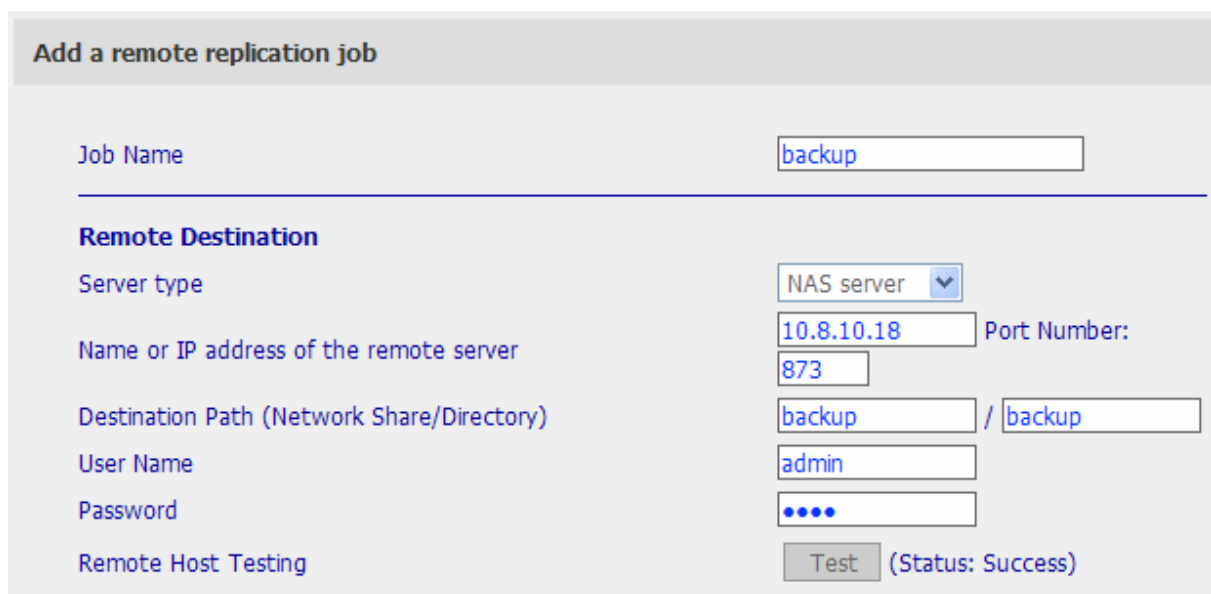


View

New Edit Delete

Job Name	Schedule	Status
There is no existing replication schedule.		

- b. Enter the job name and the remote destination settings. Select the server type. Enter the IP address or domain name (if any) of the remote server, the port number of the remote server for remote backup, the destination path, and the user name and password with write access to the remote server. Click "Test" to check if the connection is successful or not.



**Add a remote replication job**

Job Name

---

**Remote Destination**

Server type

Name or IP address of the remote server  Port Number:

Destination Path (Network Share/Directory)  /

User Name

Password

Remote Host Testing  (Status: Success)



**Note:** To use remote replication, enable Microsoft Networking service, make sure the destination network share and directory have been created, and the user name and password are valid to login the destination folder.

- Local Source**

Source Path (Network Share/Directory)  /

---

☒ Replicate Now

Replication Schedule   Hour :   Minute

☐ Daily

☐ Weekly

☐ Monthly   Day

- ☐ Enable encryption, port number:

(Note that you have to allow SSH encryption on the remote host server and the port number must be the same as the SSH port of the remote host.)

☐ Activate file compression

☐ Stop network file services while replicating

☐ Perform incremental replication

☐ Delete extra files on remote destination

View

New

Edit

Delete

	Job Name	Schedule	Status
<input type="checkbox"/>	backup	10:51 - Replicate Now	Finished(10:51 2008/10/23)

### 3.8.11 Back up/ Restore/ Reset Settings

- To back up all settings, including user accounts, server name and network configuration etc., click "Backup" and select to open or save the setting file.
- To restore all settings, click "Browse" to select a previously saved setting file and click "Restore" to confirm.
- To reset all settings to default, click "Reset".

**Caution:** When you press "Reset" on this page, all drive data, user accounts, network shares and system settings are cleared and restored to default. Please make sure you have backed up all the important data and system settings before resetting the NAS.

- Backup/ Restore/ Reset Settings

- To restore all settings, click Browse to select a previously saved setting file and click Restore to confirm.
- To backup all settings, including user accounts, server name and network configuration etc., click Backup and select to open or save the setting file.
- To reset all settings to default, click Reset.

**Caution:** When you press [Reset] on this page, all drive data, user accounts, network shares and system settings are cleared and restored to default. Please make sure you have backed up all the important data and system settings before resetting the NAS.

### 3.8.12 IP Filter

Enter the IP address or network from which the connections to this server are allowed or rejected. When the connection of a host server is denied, all protocols of that server are not allowed to access the local server.

After changing the settings, click "Apply" to save the changes. The network services will be restarted and current connections to the server will be disconnected.

- IP Filter

Security Level    Network Access Protection

Enter the IP address or network from which the connections to this server will be allowed or rejected.

☐ High - Allow connections from the list only

☐ Medium - Deny connections from the list

☒ Low - Allow all connections

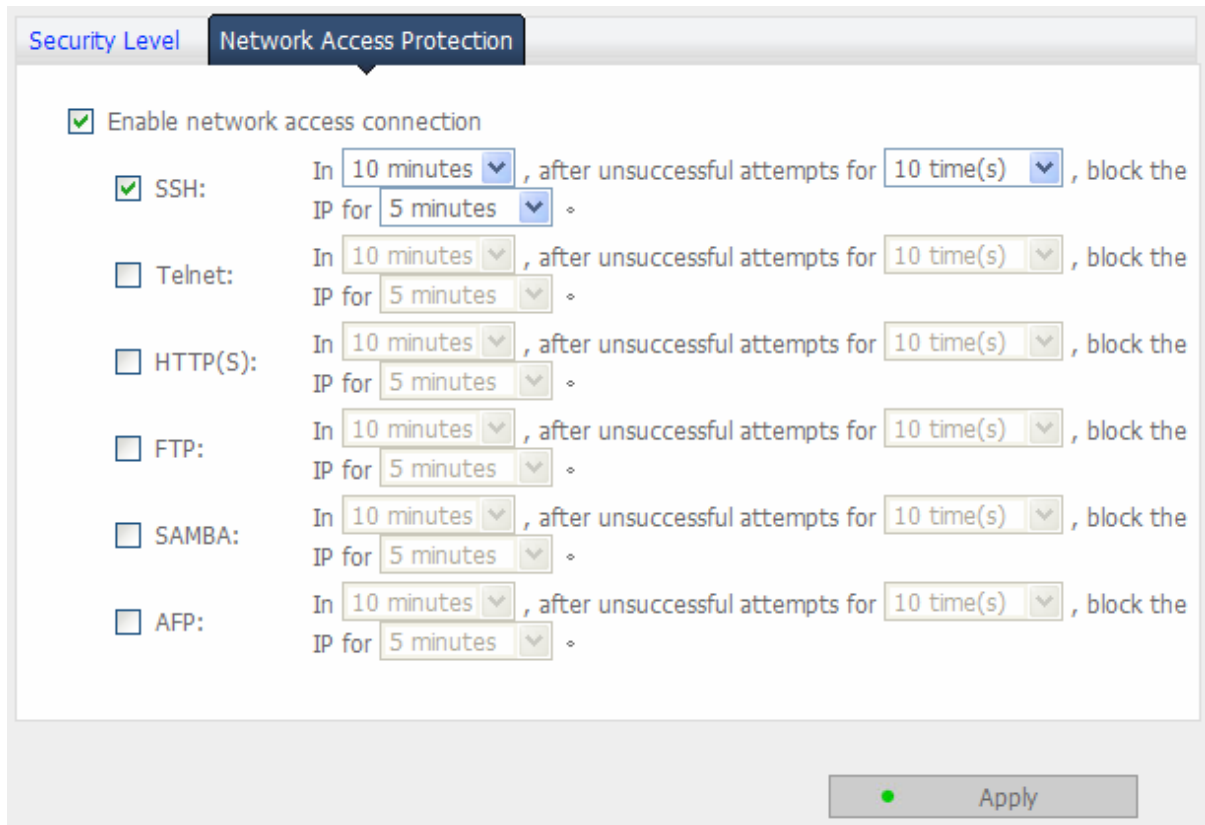
+

-

Genre	IP address or network domain	Time left for IP blockin
-------	------------------------------	--------------------------

Apply

The network access protection enhances the security of the system and prevents unwanted intrusion. You can select to block the IP for a certain period of time or forever if the IP fails to login the server from a particular connection method.



The image shows a configuration window titled "Network Access Protection" with a "Security Level" tab. The window contains a list of network access methods with checkboxes and dropdown menus for blocking IP addresses.

**Security Level** **Network Access Protection**

☒ Enable network access connection

☒ SSH: In 10 minutes, after unsuccessful attempts for 10 time(s), block the IP for 5 minutes.

☐ Telnet: In 10 minutes, after unsuccessful attempts for 10 time(s), block the IP for 5 minutes.

☐ HTTP(S): In 10 minutes, after unsuccessful attempts for 10 time(s), block the IP for 5 minutes.

☐ FTP: In 10 minutes, after unsuccessful attempts for 10 time(s), block the IP for 5 minutes.

☐ SAMBA: In 10 minutes, after unsuccessful attempts for 10 time(s), block the IP for 5 minutes.

☐ AFP: In 10 minutes, after unsuccessful attempts for 10 time(s), block the IP for 5 minutes.

Apply

### 3.8.13 Network Recycle Bin

This function enables files deleted on the shares of the NAS to be removed to Network Recycle Bin to reserve the files temporarily. To enable this function, check the box "Enable Network Recycle Bin" and click "Apply". The system creates a network share "Network Recycle Bin" automatically.

To delete all the files in network recycle bin, click "Clean Network Recycle Bin".

**Network Recycle Bin**

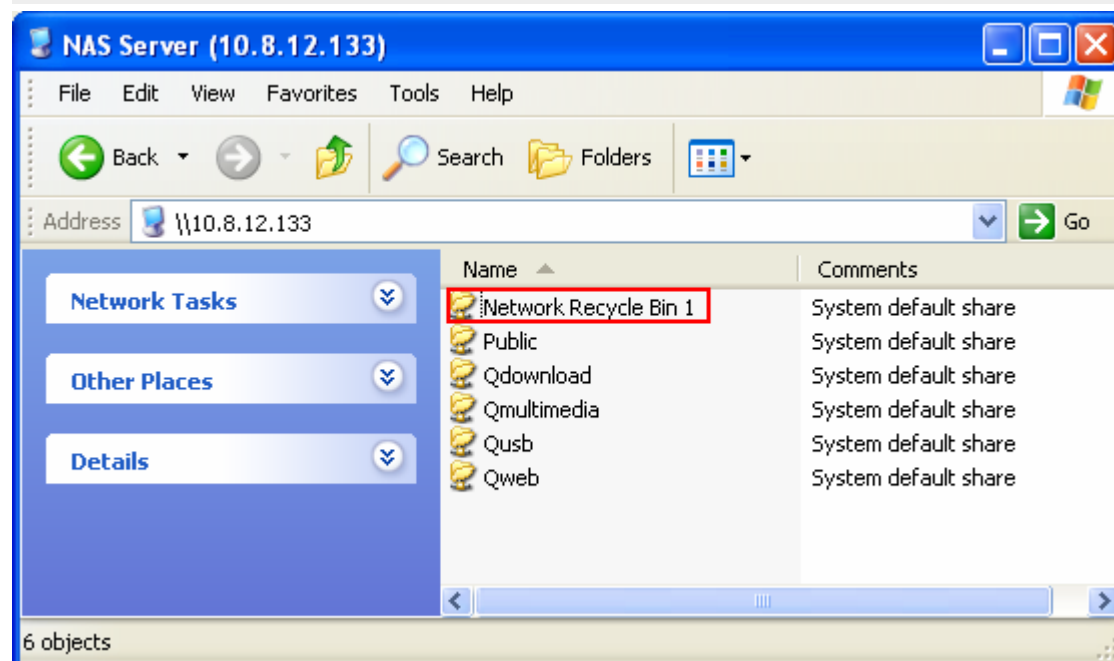
☒ Enable Network Recycle Bin

After enabling Network Recycle Bin, all the deleted files on the network folders of the NAS are moved to the "Network Recycle Bin" network folder.

Click "Clean network recycle bin" to delete all the files in network recycle bin.

[Empty Network Recycle Bin](#)

[Apply](#)



### 3.8.14 Remote Login

After enabling this option, you can access this server via Telnet or SSH encrypted connection (only the account "admin" can login remotely). You can use certain Telnet or SSH connection clients for connection, e.g., putty. Please make sure you have opened the configured ports on your router or firewall when using this function.

- Remote login

After enabling this option, you can access this server via Telnet or SSH connection. (Only the account admin can login remotely.)

☐

Allow Telnet connection

Port

13131

☒

Allow SSH connection

Port

22

Apply

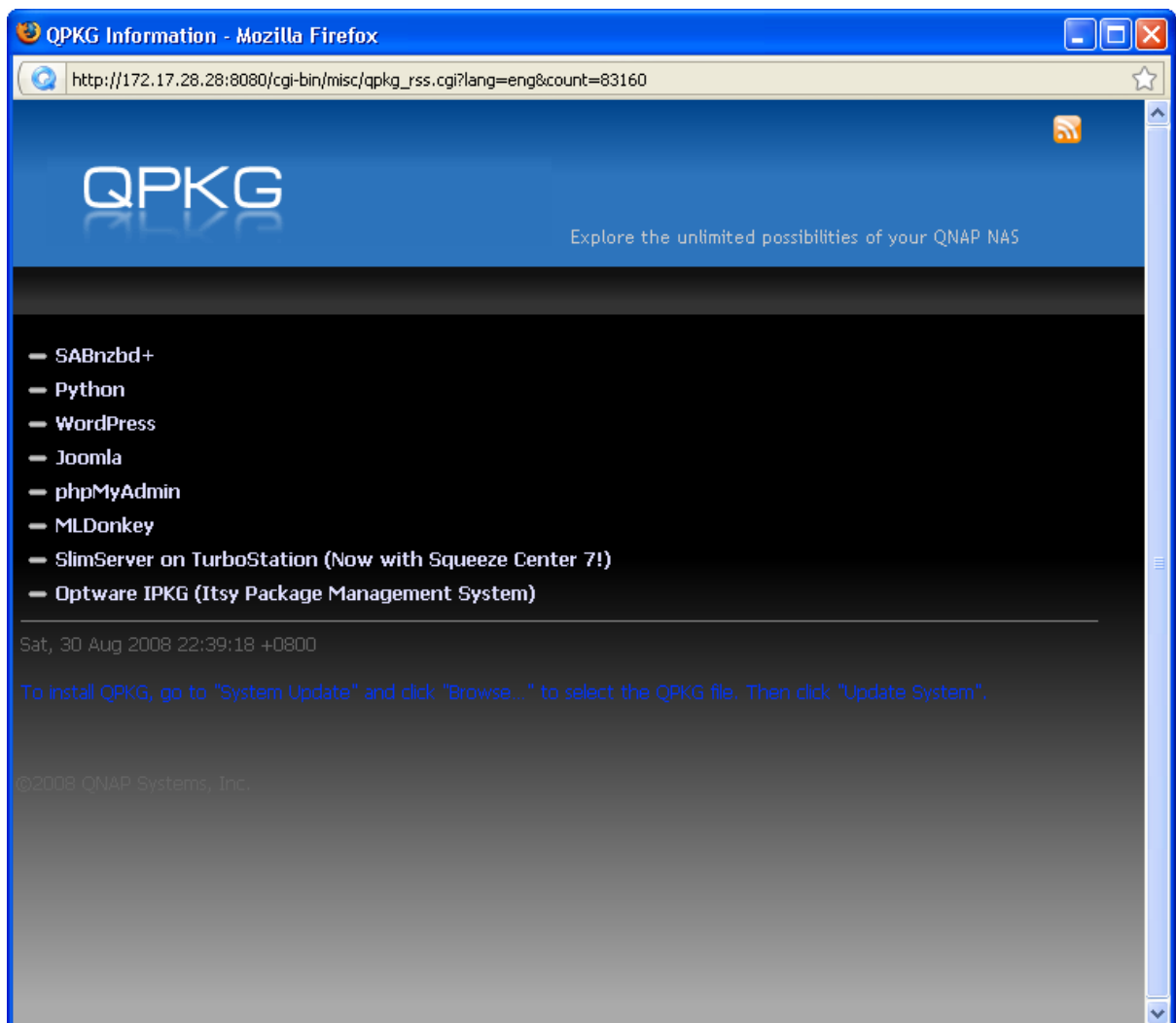


### 3.8.15 QPKG

You can install QPKG packages to add more functions to NAS. Click "Get QPKG".



Before you install the packages, make sure the files are correct, read the instructions carefully, and back up all important data on the NAS. Download the software package you want to install on NAS to your computer.



Before installing the QPKG package, please unzip the downloaded file. To install QPKG, browse to select the correct qpkg file and click "Upload".



The screenshot shows the QPKG management interface. At the top, there is a header bar with a minus sign and the text "QPKG" on the left, and a "Get QPKG" link on the right. Below the header, a light purple banner displays the message "No QPKG record found.". At the bottom, there is a text input field containing the path "C:\Documents and Settings\Admin", followed by a "Browse..." button and an "Upload" button.

After uploading the QPKG packages, the details are shown on the QPKG page. Click the link to access the web page of the installed software package and start to configure the settings. To remove the package from the NAS, click "Remove".



The screenshot shows the QPKG management interface with a package installed. The header bar is the same as in the previous screenshot. Below the header, the package name "Joomla" is listed in a blue link, with an upward-pointing arrow to its right. Below this, the package details are displayed in a table-like format:

File Name	Joomla.qpkg
Installation Date	2008-11-05
Version	1.5.1
Installation Path	/share/Qweb/Joomla
Web Page	<a href="http://172.17.21.123/Joomla/">http://172.17.21.123/Joomla/</a>
Maintainer	QNAP Systems, Inc.

At the bottom right of the details section, there is a "Remove" button.

### 3.8.16 Import SSL Secure Certificate

The Secure Socket Layer (SSL) is a protocol for encrypted communication between web servers and browsers for secure data transfer. You can upload a secure certificate issued by a trusted provider. After you have uploaded a secure certificate, you can access the administration interface by SSL connection and there will not be any alert or error message. The system supports X.509 certificate and private key only.

- Import SSL Secure Certificate

You can upload a secure certificate issued by a trusted provider. After you have uploaded a secure certificate successfully, you can access the administration interface by SSL connection and there will not be any alert or error message.

If you upload an incorrect secure certificate, you may not be able to login the server via SSL. To resolve the problem, you can restore the secure certificate to default and access the system again.

Status: Default secure certificate being used

Certificate: Please enter a certificate in X.509PEM format below.

View sample

Private Key: Please enter a certificate in X.509PEM format below.

View sample

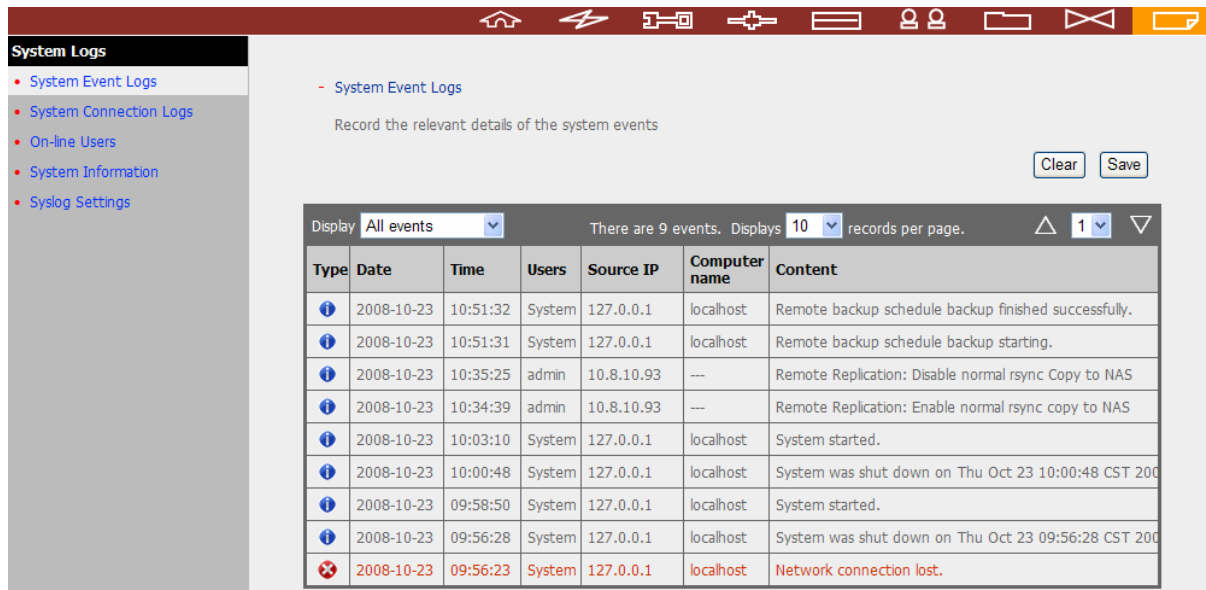
Upload

Clear

## 3.9 Event Logs

### 3.9.1 System Event Logs

The NAS can store 10,000 recent event logs, including warning, error, and information messages. In case of system malfunction, you can refer to the event logs to analyze the problems.



The screenshot displays the 'System Logs' section of a web interface. On the left, a sidebar lists navigation options: System Event Logs (selected), System Connection Logs, On-line Users, System Information, and Syslog Settings. The main area shows the 'System Event Logs' title and a description: 'Record the relevant details of the system events'. Below this, there are 'Clear' and 'Save' buttons. A table displays the event logs, with a header row and several data rows. The table includes columns for Type, Date, Time, Users, Source IP, Computer name, and Content. The events listed include backup completion, backup starting, remote replication status changes, system start/shutdown, and a network connection loss.

Type	Date	Time	Users	Source IP	Computer name	Content
Information	2008-10-23	10:51:32	System	127.0.0.1	localhost	Remote backup schedule backup finished successfully.
Information	2008-10-23	10:51:31	System	127.0.0.1	localhost	Remote backup schedule backup starting.
Information	2008-10-23	10:35:25	admin	10.8.10.93	---	Remote Replication: Disable normal rsync Copy to NAS
Information	2008-10-23	10:34:39	admin	10.8.10.93	---	Remote Replication: Enable normal rsync copy to NAS
Information	2008-10-23	10:03:10	System	127.0.0.1	localhost	System started.
Information	2008-10-23	10:00:48	System	127.0.0.1	localhost	System was shut down on Thu Oct 23 10:00:48 CST 2008
Information	2008-10-23	09:58:50	System	127.0.0.1	localhost	System started.
Information	2008-10-23	09:56:28	System	127.0.0.1	localhost	System was shut down on Thu Oct 23 09:56:28 CST 2008
Error	2008-10-23	09:56:23	System	127.0.0.1	localhost	Network connection lost.

### 3.9.2 System Connection Logs

The system supports logging HTTP, FTP, Telnet, SSH, AFP, NFS, SAMBA, and iSCSI connections. Click "Options" to select the connection type to be logged.

The file transfer performance can be slightly affected by enabling the event logging.

**Tip:** You can right click the log on the list of connection logs and select to delete the record or add the IP to banned list and select how long the IP should be banned.

- System Connection Logs

Record the logs of connections to the system

Status: Logging

OptionsStop loggingClearSave

Display All events ▼

There are 33 events. Displays 10 ▼ records per page.

△ 1 ▼ ▽

Type	Date	Time	Users	Source IP	Computer name	Connection type	Accessed resources	Action
ⓘ	2008			10.8.10.12	---	HTTP	Administration	Login OK
ⓘ	2008					HTTP	Administration	Login OK
ⓘ	2008-12-16	10:06:45	admin			HTTP	Administration	Login OK
ⓘ	2008-12-16	09:58:46	admin			HTTP	Administration	Login OK
ⓘ	2008-12-16	09:56:50	admin			SSH	---	Login OK
ⓘ	2008-12-15	19:31:49	admin			SSH	---	Logout

Delete this record

Add to the block list ▶

5 minutes

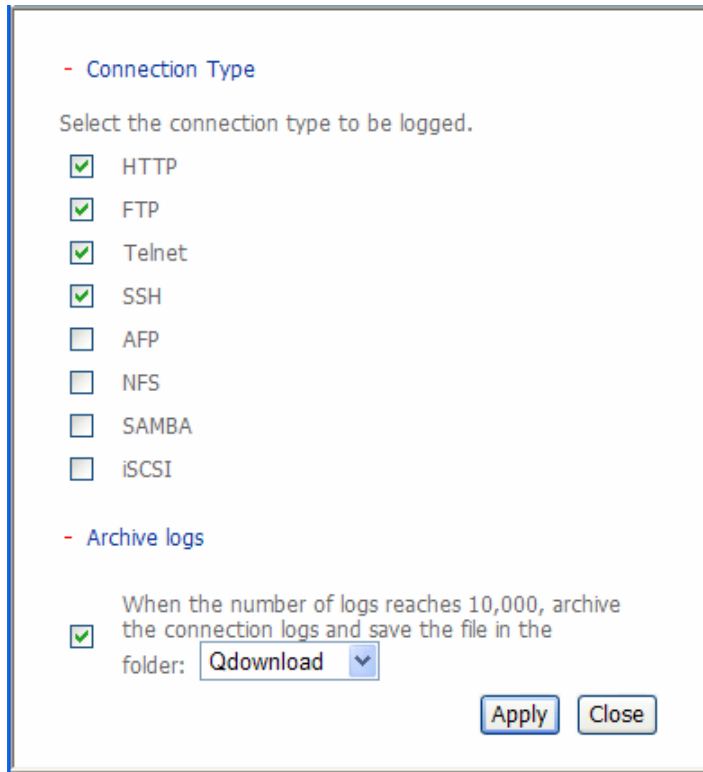
30 minutes

1 hour

1 day

forever

Archive logs: Enable this option to archive the connection logs. The system generates a csv file automatically and saves it to a specified folder when the number of logs reaches the upper limit.



The screenshot shows a configuration window with two main sections: "Connection Type" and "Archive logs".

**- Connection Type**

Select the connection type to be logged.

- ☒ HTTP
- ☒ FTP
- ☒ Telnet
- ☒ SSH
- ☐ AFP
- ☐ NFS
- ☐ SAMBA
- ☐ iSCSI

**- Archive logs**

When the number of logs reaches 10,000, archive the connection logs and save the file in the folder: ☒

### 3.9.3 On-line Users

The information of the on-line users accessing the system via networking services is shown on this page.

— On-line users

Display the information of the on-line users accessing the system via networking services







There are 2 events.

Date	Time	Users	Source IP	Computer name	Connection type	Accessed resources
2007-10-19	16:10:24	admin	10.8.12.17	---	HTTP	Administration
2007-10-19	17:05:40	admin	10.8.12.32	---	HTTP	Administration

### 3.9.4 System Information

You can view the system information, e.g., CPU usage and memory on this page.

— System Information

CPU Usage	2.7 %	CPU Temperature	28°C/82°F	
Total Memory	1008.7MB	System temperature	36°C/96°F	
Free Memory	972.8MB	HDD 1 temperature	--	
Packets Received	76185	HDD 2 temperature	38°C/100°F	
Packets Sent	23541	HDD 3 temperature	41°C/105°F	
Error Packets	0	HDD 4 temperature	38°C/100°F	
System Up Time	1Day(s)2Hour(s)35Minute(s)	System fan speed	1073 RPM	

### 3.9.5 Syslog Settings

Syslog is a standard for forwarding log messages in an IP network. You can enable this option to save the event logs and connection logs to a remote syslog server.

- Syslog Settings

☒ Enable syslog

You can enable this option to save the event logs and connection logs to a remote syslog server.

Syslog Server IP:

UDP Port:

Select the logs to record

☒ System Event Logs

☐ System Connection Logs (You must enable system connection logs to use this option.)

Apply

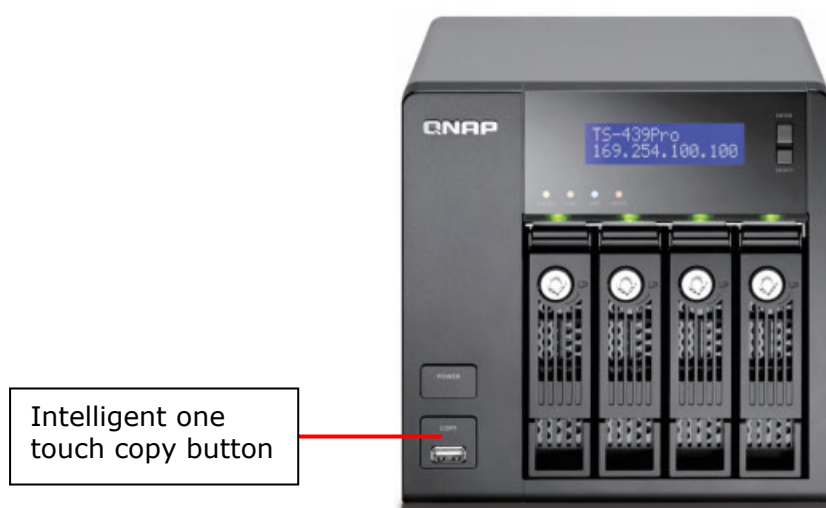


## Chapter 4. Use Front USB Backup Button

By connecting an external storage device to the NAS, you can use the front USB backup button to copy data from the external device to NAS or from the NAS to the external device. To use this function, please follow the steps below:

1. Make sure a SATA disk is installed correctly in the NAS.
2. Turn on the NAS.
3. Go to "System Tools>USB one touch copy backup" to configure the settings.
4. Connect USB devices, e.g. digital camera, flash, external USB drive to the front USB port of the NAS.
5. Press the copy button on the NAS. The data is copied according to your settings in System Tools>USB one touch copy backup.

#Intelligent one touch copy button: The NAS detects the data in the connected source automatically. The first time a USB device is connected, press the button and the NAS copies all data in the device automatically. When the same device is connected again and there are changes to the source data, press the button and the NAS copies all files in the device. If there are no changes, press the button and the NAS does not copy the files.



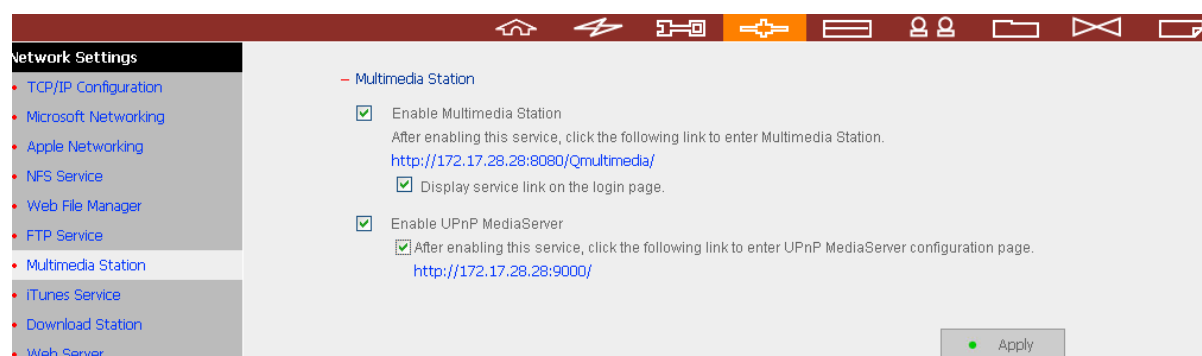
## Chapter 5. Multimedia Station

### 5.1 Share Photos and Multimedia Files via Web Interface

The NAS provides a user-friendly web management interface for you to manage personal albums easily. You can view the images and the multimedia files, or browse the photos by thumbnails preview.

#### A. Upload photos by web administration

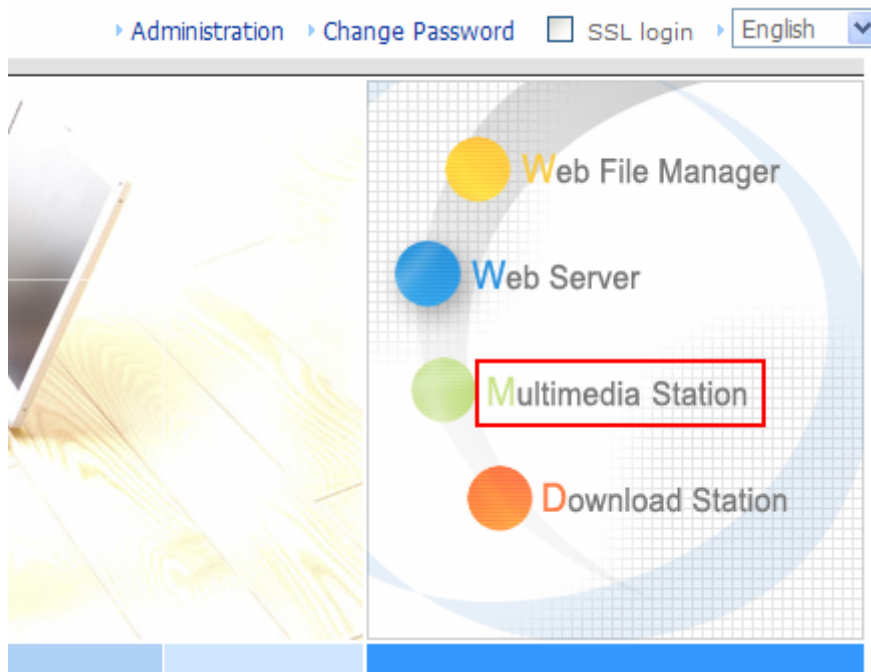
1. To use Multimedia Station, make sure a SATA disk is installed correctly. A share folder **Qmultimedia** will be created after the disk is initialized. Enable Multimedia function in **Network Settings**.




2. Click the link <http://NAS IP/Qmultimedia> on the Multimedia Station page or click "Multimedia Station" on the login page to access Multimedia Station.



**Note:** To display the Multimedia Station link on the login page, please enable the option "Display service link on the login page".




3. Click  or "Login" on the top right hand corner. Login with the administrator name and password to manage Multimedia Station. Users without administration right can view the photos and multimedia files on Multimedia Station but they do not have the right to modify the files. When logging in as Multimedia Station user, you can access the files and folders that you have authority to browse.



4. Click "Browse" to select the multimedia file and then click "Upload" to upload the file to the folder.

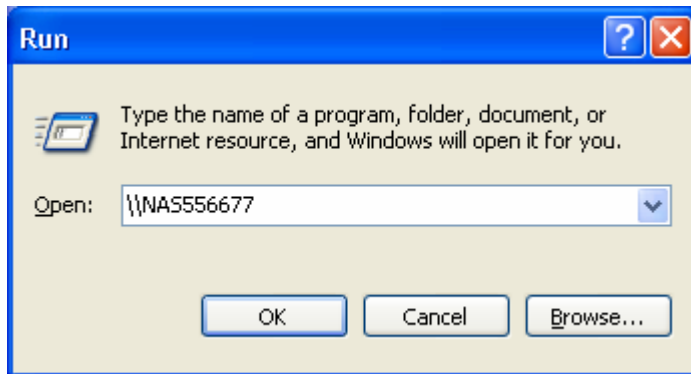


5. You can also create folders by clicking  .

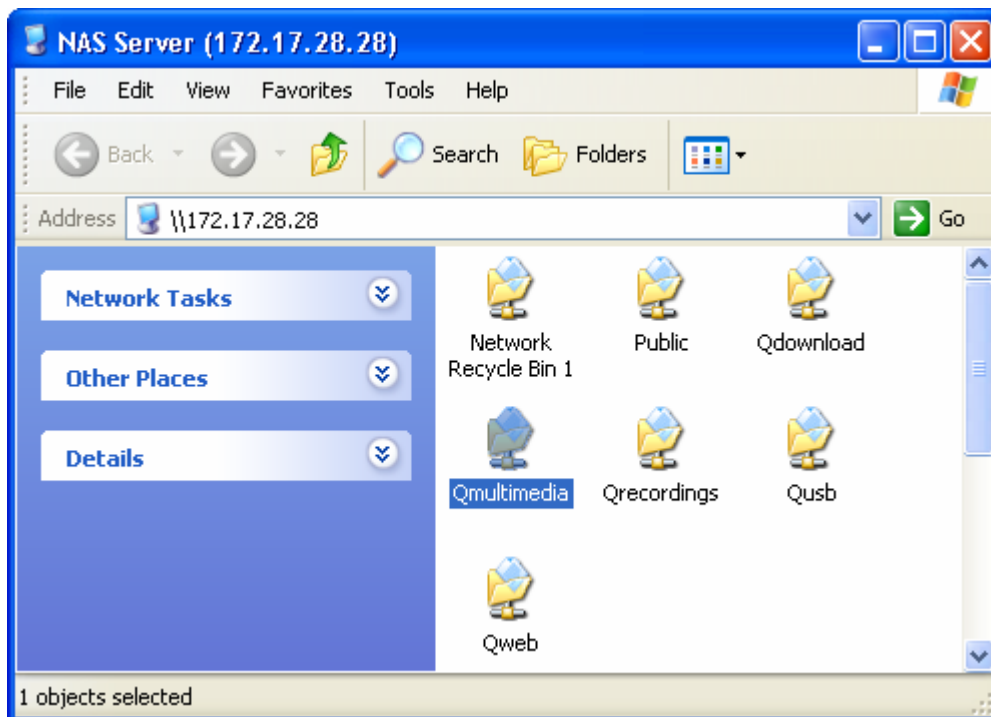
## B. Upload photos to Qmultimedia folder directly

You can upload multimedia files to the NAS directly by the following steps.

1. Use **Run** function in Windows. Enter \\[server name] or \\[server IP] to access share folder on the NAS.



2. Open the folder **Qmultimedia**. Enter the user name and password to login.



3. Drag the files and folders to the folder directly. Please wait patiently when the NAS is generating thumbnails for images during uploading.

When you login Multimedia Station by web browser again, all multimedia files are shown.



### Buttons on Multimedia Station page

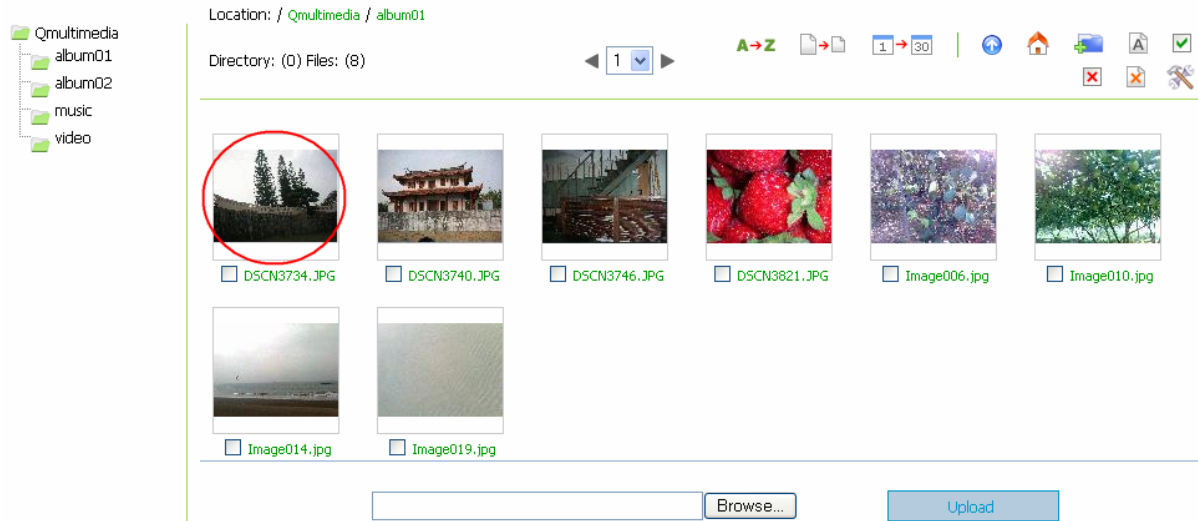
	Sort files by name
	Sort files by size
	Sort files by date
	Return to previous page
	Return to Home
	Create folder
	Rename file or folder
	Select all
	Select none
	Delete

### Support file format list

Type	File format
Picture	jpg, bmp, gif
Video	wmx, wvx, avi, mpeg, mpg, mpe, m1v, mp2, mpv2, mp2v, mpa, dvr-ms, asf, asx, wpl, wm, wmx, wmd, wmz
Audio	wma, wax, cda, wav, mp3, m3u, mid, midi, rmi, aif, aifc, aiff, au, snd
Others	(Other formats not mentioned above)

## View Photo Information

1. To view detailed information of a photo, click the thumbnail of the picture.















2. The information of the photo, e.g. file name, resolution, size, camera producer is shown on the right. You can enter a description for the picture in the box below the photo and click "Submit". To reset the description to previously saved version, click "Reset".



## Buttons Description

You can use the buttons on top of the photo to manage the album.

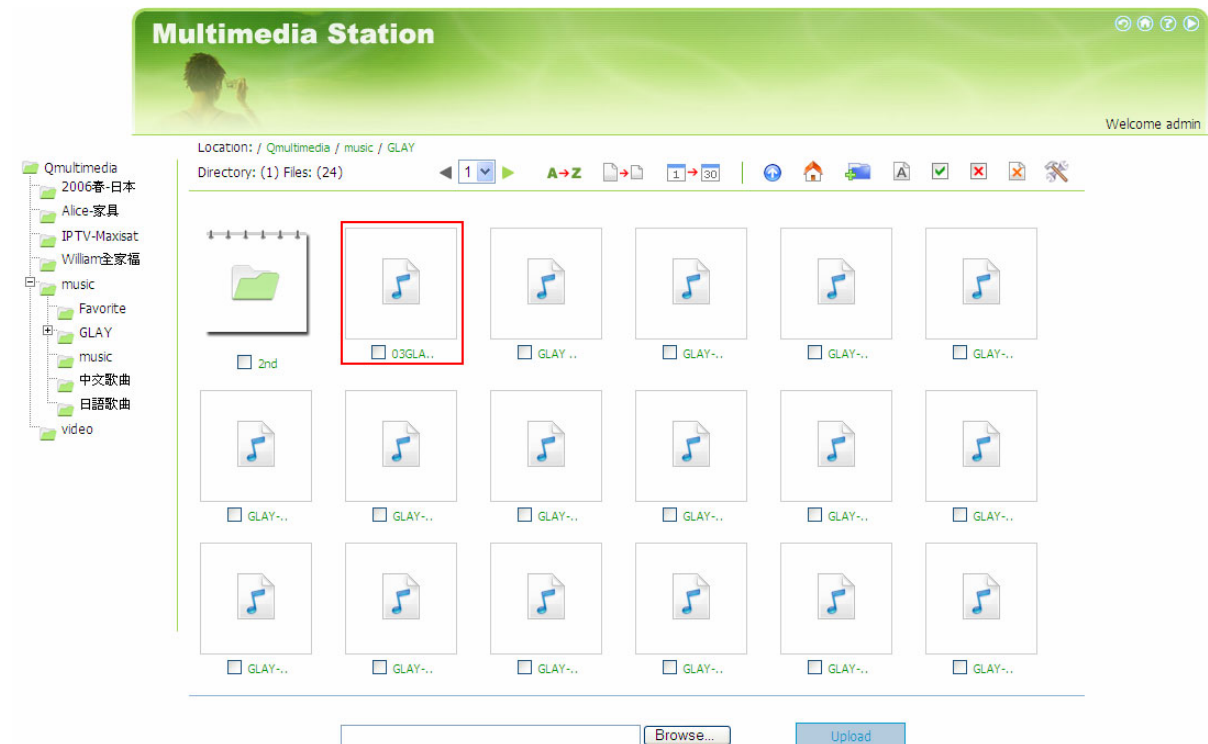
	Back to previous level
	Previous image
	Next image
	Rotate image anticlockwise
	Rotate image clockwise
	Zoom in
	Zoom out
SlideShow: <input type="text" value="3"/>  	Play slideshow. Select the time interval in seconds. Click "play" to play slide show. To stop playing, click "stop".
	Print the image
	Save the picture
	Set the picture as album cover




## Play music or video files

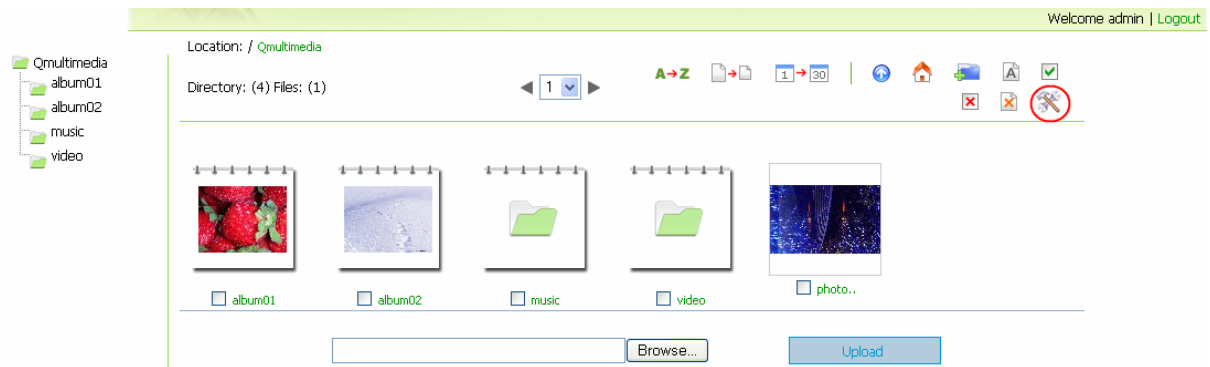
To play music or video files on Multimedia Station, you can click the thumbnail of the file displayed on the page. The file is played by the default music or video playing program of your PC.


\*It is recommended to use Media Player 10.0 or above as the default playing program.





## C. Configure album authority

1. After logging in as administrator (admin), click  to enter the configuration page for album authority.






2. You can view, add, delete, and edit users. For any inquiries when using these functions, click the help button  on the top right corner of the page.

User list [Create user](#)  

User list

User name	Status	Maintain	Description
guest	Enable	---	System default user; you can set the authority of the guests for browsing the album.
test	Enable	Delete	
user01	Enable	Delete	general user

3. You can edit user profile and album access authority on this page. For any inquiries when using these functions, click the help button  on the top right corner of the page.

Edit personal profile  

---

User's profile

User name:

Description:

Password:

Verify Password:

☐ User cannot change the information.

☐ Disable

Accessible albums

album01  
album02

← Add

Remove →

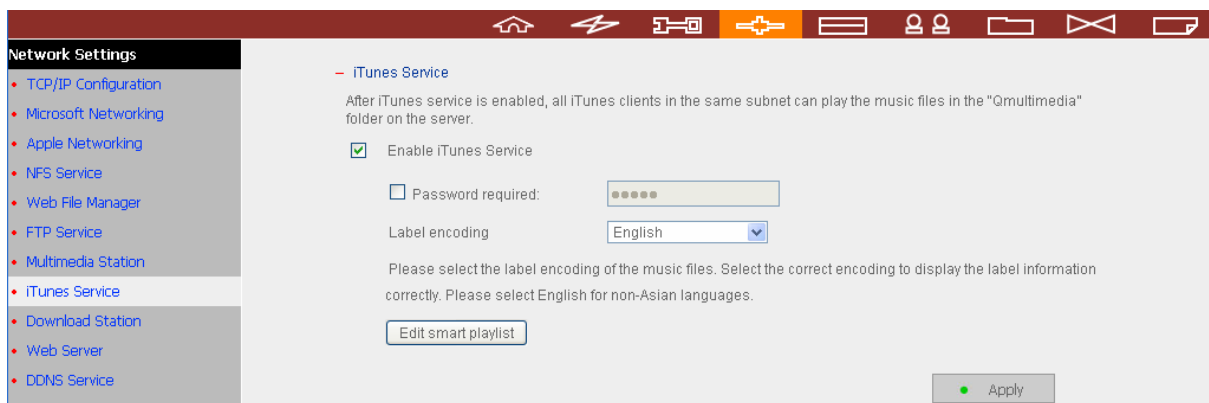
Inaccessible albums

music  
video

## 5.2 Enable iTunes Service

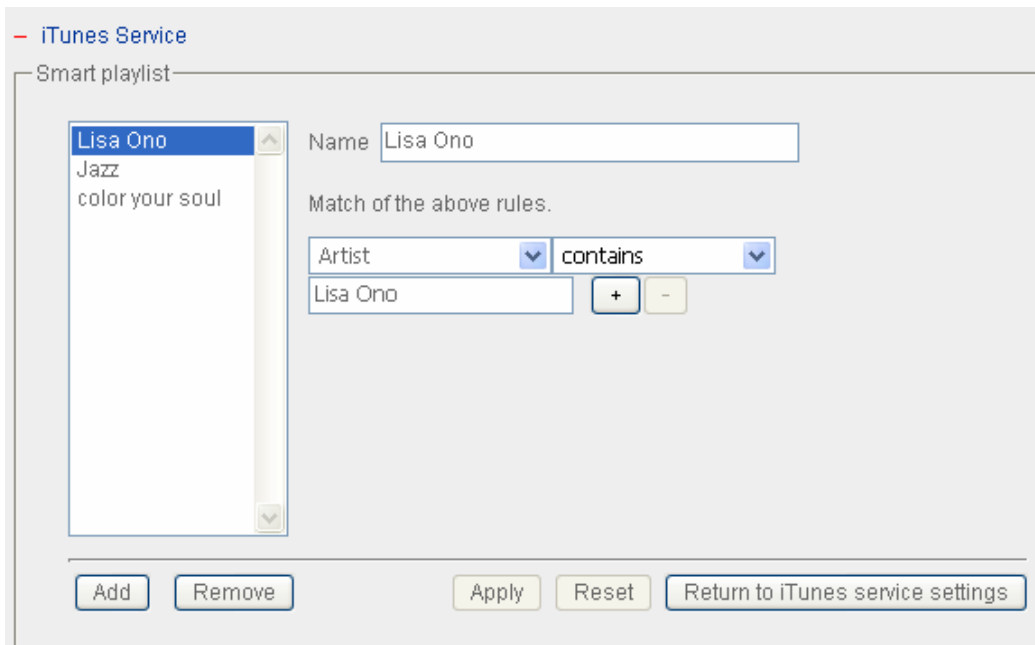
The mp3 files on Qmultimedia folder of the NAS can be shared to iTunes by enabling this service. All the computers with iTunes installed on LAN are able to find, browse, and play the music files on the NAS.

To use the iTunes service, make sure you have installed the iTunes program on your computer. Go to "Network Settings" > "iTunes Service" and enable the service. Then upload the music files to the Qmultimedia folder of NAS.



**Password required:** To allow the users to access the data only by entering the correct password, check this option and enter the password.

Click "Edit smart playlist" to enter the smart playlist page. You can define the playlist rules to categorize the songs into different playlists. If there is no song that matches the rules in the playlist, the iTunes client will not show the playlist. For detailed operation, please refer to the online help.



When you open iTunes, it detects the NAS automatically. All the songs on the Qmultimedia folder will be shown.



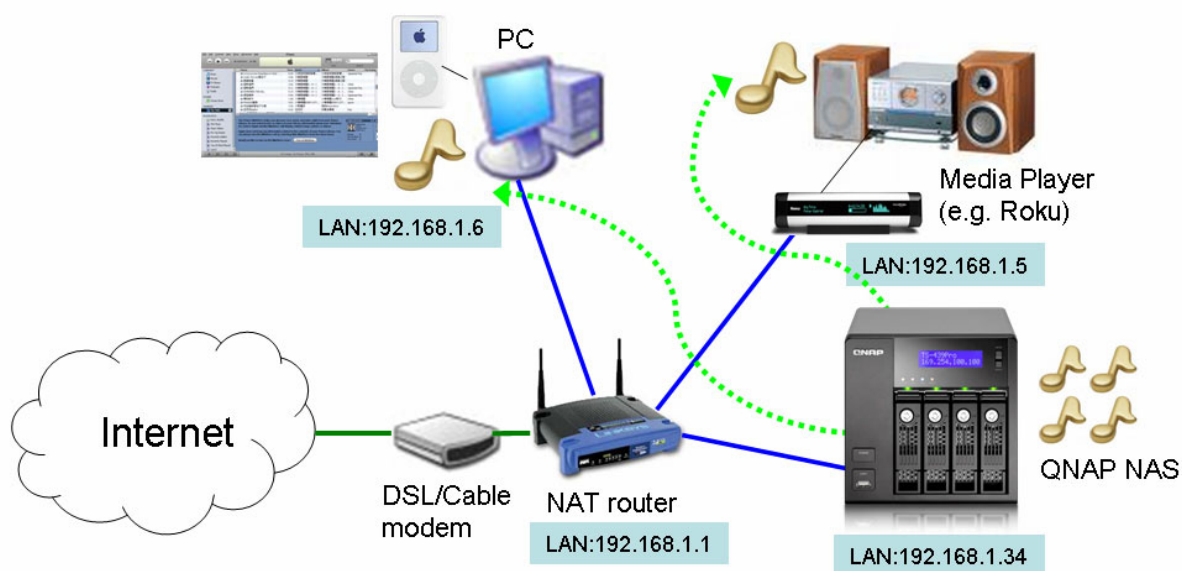
Click the triangle icon next to the NAS name. The smart playlists defined earlier will be shown. The songs are categorized accordingly. You can start to use iTunes to play the music on your NAS.



**Note:** You can download the latest iTunes software from official Apple website <http://www.apple.com>.

## 5.3 Use UPnP Media Server

The NAS is built-in with TwonkyMedia, DLNA compatible UPnP media server. Enable this function and the NAS shares particular music, photos or video files to DLNA network. You can use DLNA compatible digital media player (DMP), to play the multimedia files on the NAS on TV or acoustic sound system.



To use UPnP Media Server, enable this function and click the following link ([http://NAS IP:9000/](http://NAS_IP:9000/)) to enter the configuration page of UPnP Media Server.

— Multimedia Station

☒ Enable Multimedia Station  
After enabling this service, click the following link to enter Multimedia Station.  
<http://172.17.20.5:8080/Qmultimedia/>  
☐ Display service link on the login page.

☒ Enable UPnP MediaServer  
☒ After enabling this service, click the following link to enter UPnP MediaServer configuration page.  
<http://172.17.20.5:9000/>

● Apply

Click the link <http://NAS IP:9000/> to enter UPnP Media Server configuration page and configure the following settings.

- (1) Language: Select the display language.
- (2) Server Name: Enter the name of the NAS UPnP Media Server. This name is shown on DMP operation interface, e.g. NAS.
- (3) Content Locations: Select the share folder on the NAS to be shared to DMP. The default folder is Qmultimedia. You can add more than one share folder.

Click "Save Changes" to save the settings.

After configuring the settings, you can upload mp3, photos, or video files to Qmultimedia folder or other specified folders on the NAS.



**Note:** If you upload multimedia files to the default share folder but the files are not shown on Media Player, you can click "Rescan content directories" or "Restart server" on the Media Server configuration page.

The built-in UPnP Media Server of the NAS is compatible with the DLNA DMP devices in the market.



## **About UPnP and DLNA**

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. The purpose of UPnP is to allow devices to connect seamlessly and to simplify the implementation of networks at home and in corporate environment. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.

The term UPnP is gleaned from Plug-and-play, a technology for dynamically attaching devices to a computer directly.

The Digital Living Network Alliance (DLNA) is an alliance of a number of consumer electronics, mobile and personal computer manufacturers. Its aim is to establish a home network in which the electronic devices from all companies are compatible with each other under an open standard. The alliance also tries to promote the idea of digital home by establishing DLNA certification standard. All DLNA certified products connected to the home network can be accessed seamlessly to enable consumers to enjoy digital life conveniently.

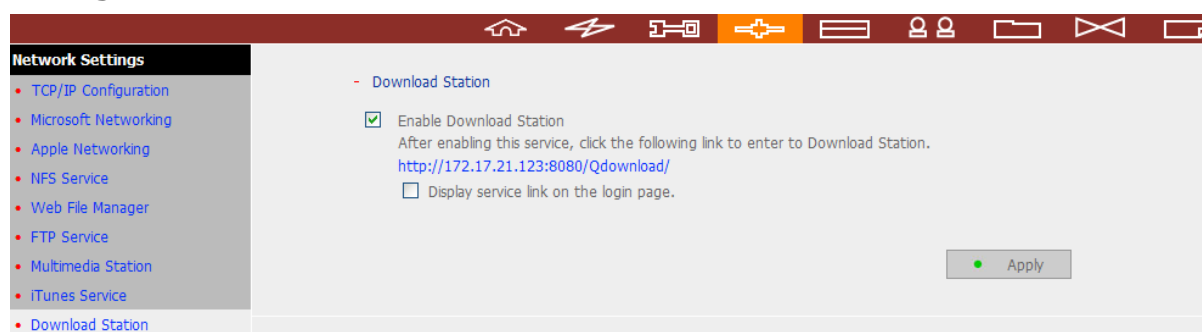
## Chapter 6. Download Station

The NAS supports BT, HTTP, and FTP download mechanism. You can add download task to the NAS and let the server finish downloading independent of PC.



**Warning:** Please be warned against illegal downloading of copyrighted materials. The Download Station functionality is provided for downloading authorized files only. Downloading or distribution of unauthorized materials may result in severe civil and criminal penalty. Users are subject to the restrictions of the copyright laws and should accept all the consequences.

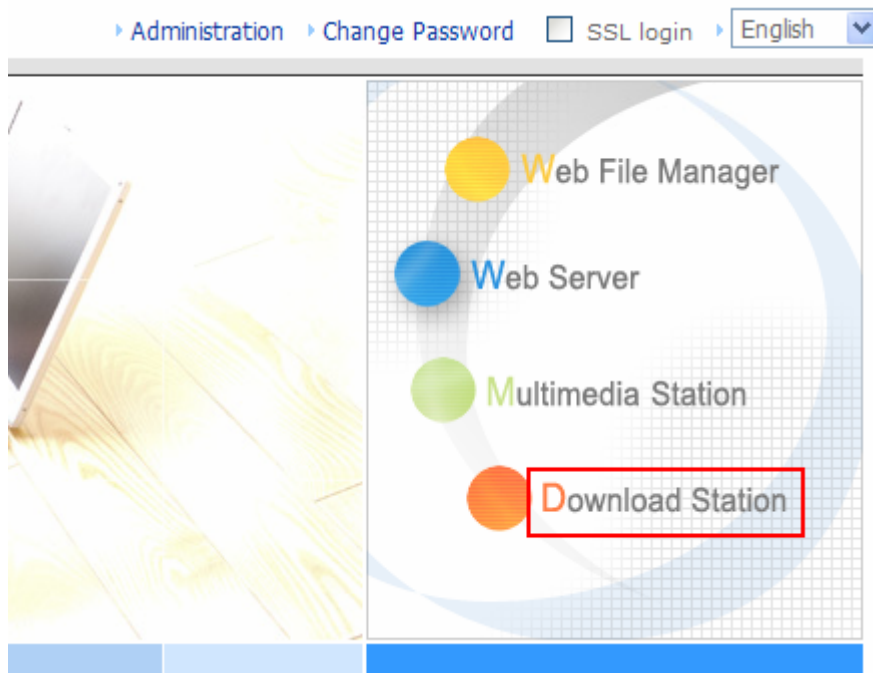
1. To use Download Station, make sure one or two SATA disks are installed correctly in the NAS. A share folder **Qdownload** is created. Enable this function in **Network Settings**.



2. Click the link <http://NAS IP/Qdownload> on Download Station page or click "Download Station" on the login page of the NAS to access Download Station.



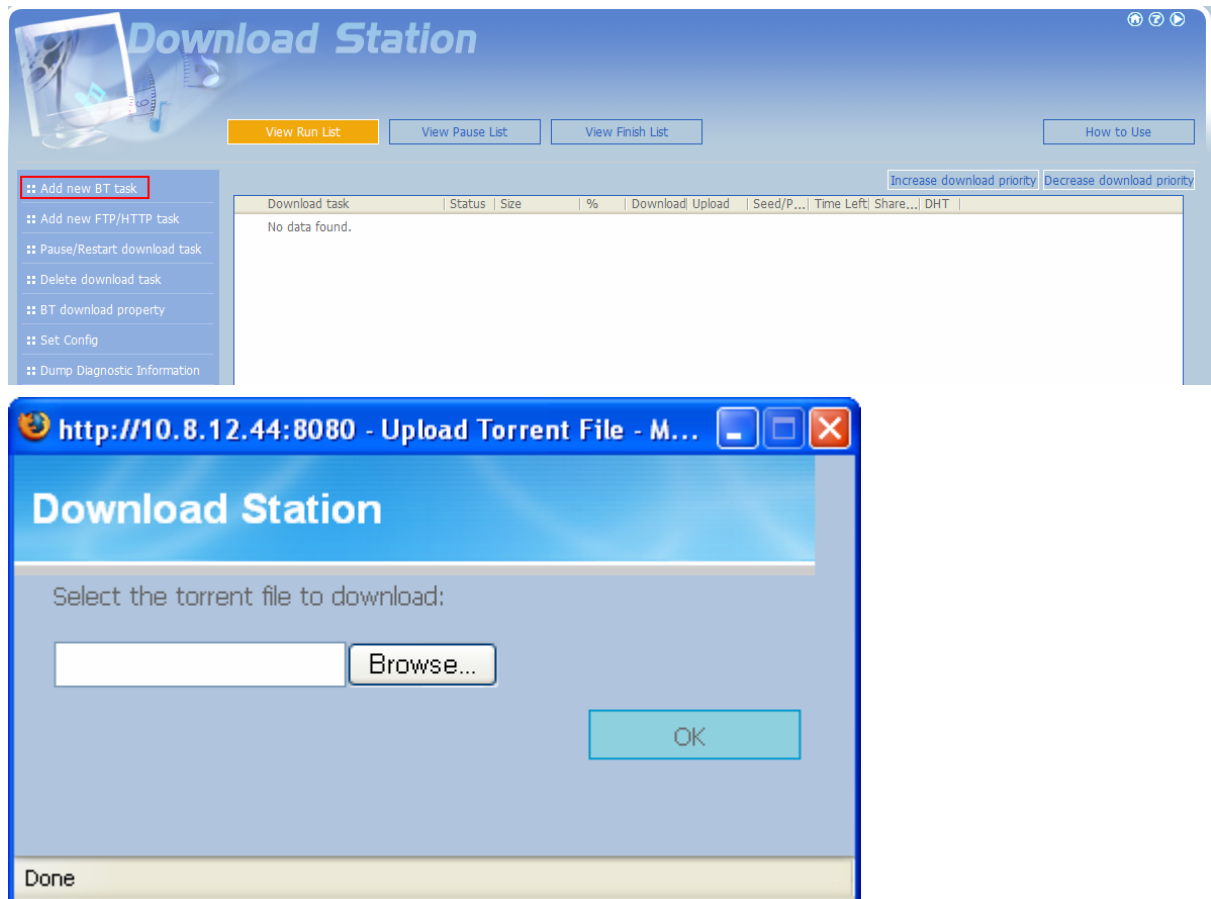
**Note:** To display the Download Station link on the login page, please enable the option "Display service link on the login page".



3. Select **Add new BT task** or **Add new FTP/HTTP task**.

**(A) Add new BT task**

Click "Add new BT task" on the left and upload a torrent file. You can download legal torrent files by searching on the Internet. There are websites that provide legally sharing torrents e.g. [www.legaltorrents.com](http://www.legaltorrents.com). Please download the torrent files to your local disk and then upload them to the NAS.



### (B) Add new FTP/HTTP task

To run an FTP download task, click "Add new FTP/HTTP task". Enter the FTP URL of the download task and select the share folder to save the files. Enter the user name and password to login the FTP server (if necessary). Then click "OK" to start downloading.

To run an HTTP download task, click "Add new FTP/HTTP task". Enter the HTTP URL of the download task and select the share folder to save the files. Then click "OK" to start downloading.

The screenshot shows a window titled "http://10.8.12.44:8080 - Add New FTP/HTTP Tas...". The main heading is "Download Station". Below it, the text "Add new FTP/HTTP task" is displayed. The form contains the following fields and controls:

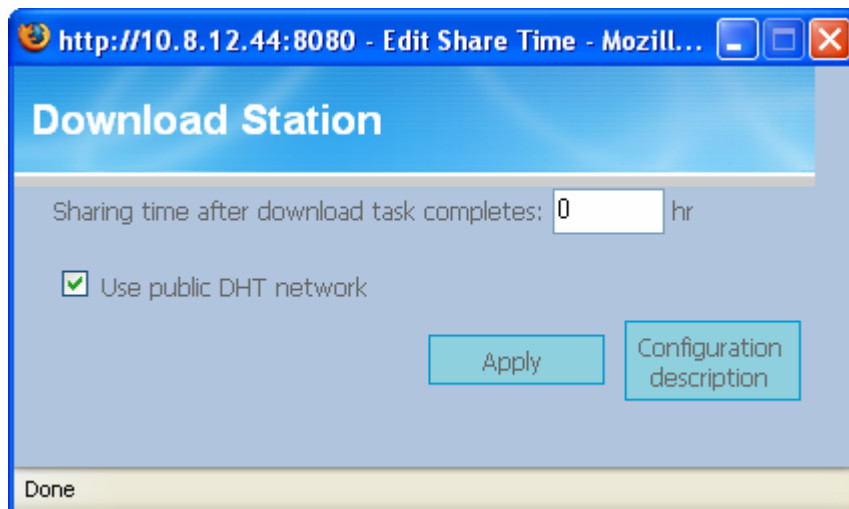
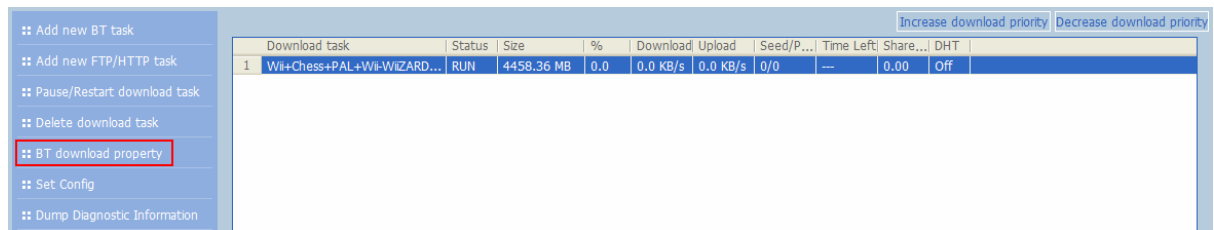
- "Input URL of the download task:" with a text box containing "ftp://".
- "Save to network share folder:" with a dropdown menu showing "Qdownload".
- An unchecked checkbox labeled "Input the user name and password for the URL of the download task:".
- "User name:" and "Password:" text boxes.
- "OK" and "Configuration description" buttons.
- A "Done" button at the bottom left.

4. After uploading a download task, the task appears on **View Run List**.

The screenshot shows the "View Run List" tab in the Download Station software. The interface includes a sidebar with various options and a main table displaying the current download task.

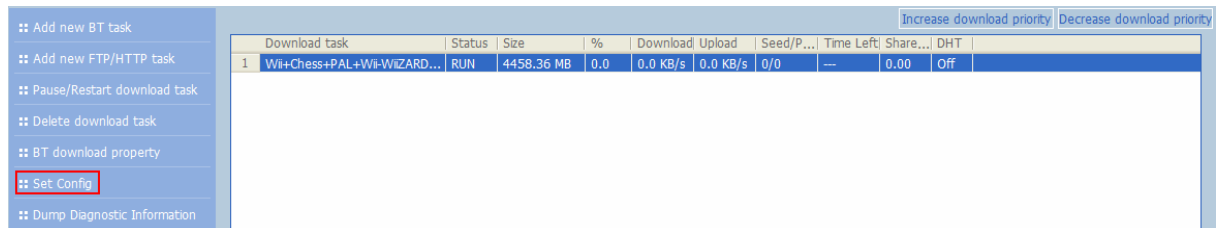
Download task	Status	Size	%	Download	Upload	Seed/P...	Time Left	Share...	DHT
1 Wi+Chess+PAL+Wi-WIZARD...	RUN	4458.36 MB	0.0	0.0 KB/s	0.0 KB/s	0/0	---	0.00	Off

5. You can select a download task and click “BT download property” to enable or disable DHT public network and configure the sharing time after download completes.



**Note:** If the sharing time (larger than 0 hr) is set for a download task, the download task will be moved to Finish List after download completes and the sharing time ends.

- Click "Set Config" and enter the number of the maximum tasks you want to download at the same time (Default number: 3).  
Enter the maximum download rate (default value is 0, which means unlimited).  
Enter the maximum upload rate (default value is 0, which means unlimited).  
Enter the port range for Download Station (default range is 6881-6999).  
Check UPnP NAT port forwarding to enable automatically port forwarding on UPnP supported gateway (default is not checked).



## Download Station

Maximum number of downloads at the same time:

☒ When the total number of records on all the lists reaches the upper limit, overwrite the oldest records on the "Finish List".

Maximum download rate (KB/s):   
(default value is 0, which means unlimited)

Maximum upload rate (KB/s):   
(default value is 0, which means unlimited)

BitTorrent port range:  -

☐ UPnP NAT port forwarding

☐ Protocol encryption

### Protocol Encryption

There are a number of Internet Service Providers (ISP) block or throttle BitTorrent connections for the high bandwidth it generates. By turning on "Protocol Encryption" your connections will not be distinguished by these ISPs as BitTorrent connections therefore are unable to block or throttle them and causing slow connections or even no connections. However some ISPs are starting to be able to identify these connections even if they were encrypted so users are suggested to check the Bad ISPs list on AzureusWiki and to consider switching to an ISP that does not perform BitTorrent traffic throttling or blocking.

You can set the download schedule in "Download time settings". Select "Continuous download" to download the files continuously. To specify the download schedule, select "Daily download time" and enter start and end time. If the end time value is smaller than the start time, the end time will be treated as the time on the next day.

Download time settings:

☐ Continuous download

☒ Daily download time:

☒ 18 : 00 ~ 07 : 00

☐ 00 : 00 ~ 00 : 00

Apply Configuration description

- To pause a running download task, select the task in **View Run list** and click "Pause/ Restart download task". You can view the tasks that are paused or finished in View Pause List and View Finish List respectively. To restart a paused task, select the task in **View Pause List** and click "Pause/ Restart download task".

Left sidebar menu:

- :: Add new BT task
- :: Add new FTP/HTTP task
- :: Pause/Restart download task**
- :: Delete download task
- :: BT download property
- :: Set Config
- :: Dump Diagnostic Information

Right sidebar buttons: Increase download priority Decrease download priority

Download task	Status	Size	%	Download	Upload	Seed/P...	Time Left	Share...	DHT
1 Wi+Chess+PAL+Wi-WiZARD...	RUN	4458.36 MB	0.0	0.0 KB/s	0.0 KB/s	0/0	---	0.00	Off

- You can also increase or decrease task priority by clicking "Increase download priority" and "Decrease download priority" when there are multiple download tasks.

Left sidebar menu:

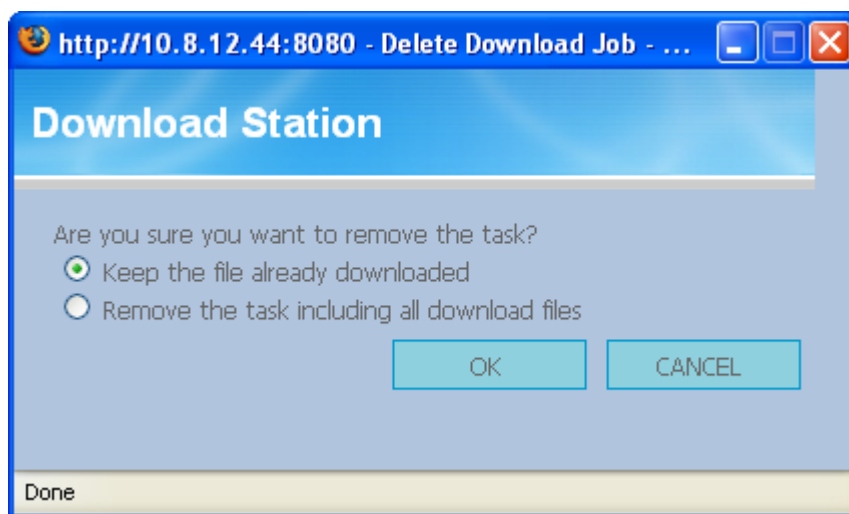
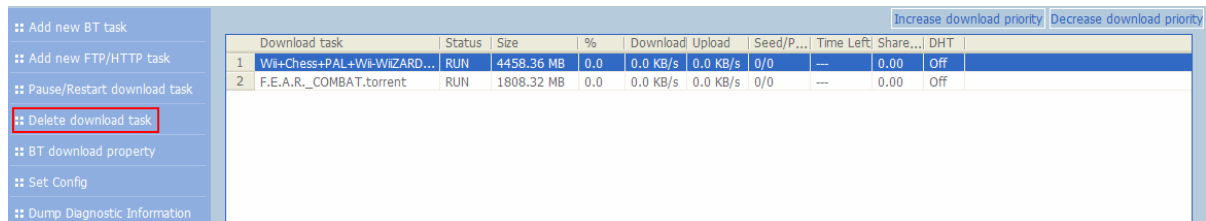
- :: Add new BT task
- :: Add new FTP/HTTP task
- :: Pause/Restart download task
- :: Delete download task
- :: BT download property
- :: Set Config
- :: Dump Diagnostic Information


Right sidebar buttons: Increase download priority Decrease download priority

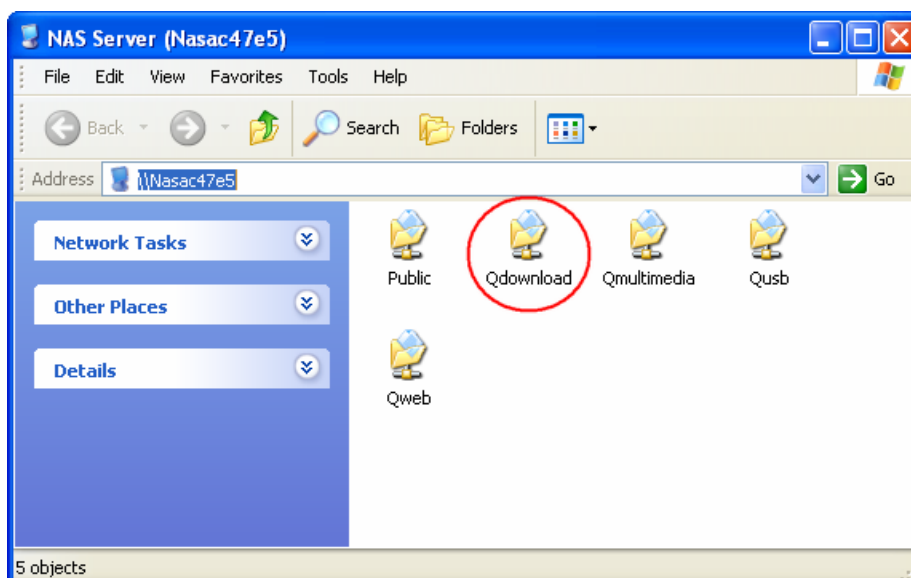
Download task	Status	Size	%	Download	Upload	Seed/P...	Time Left	Share...	DHT
1 Wi+Chess+PAL+Wi-WiZARD...	RUN	4458.36 MB	0.0	0.0 KB/s	0.0 KB/s	0/0	---	0.00	Off
2 F.E.A.R._COMBAT.torrent	RUN	1808.32 MB	0.0	0.0 KB/s	0.0 KB/s	0/0	---	0.00	Off



9. To delete a running, paused, or finished task, select the task and click "Delete download task". You can select to remove the download task only and retain the downloaded files, or remove the task and downloaded files.

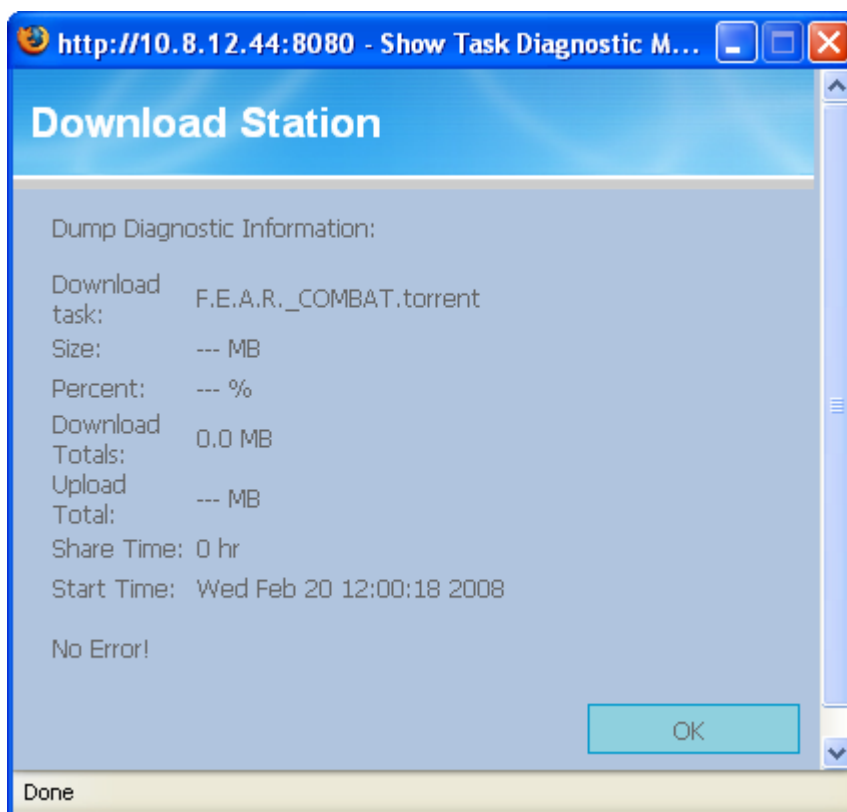
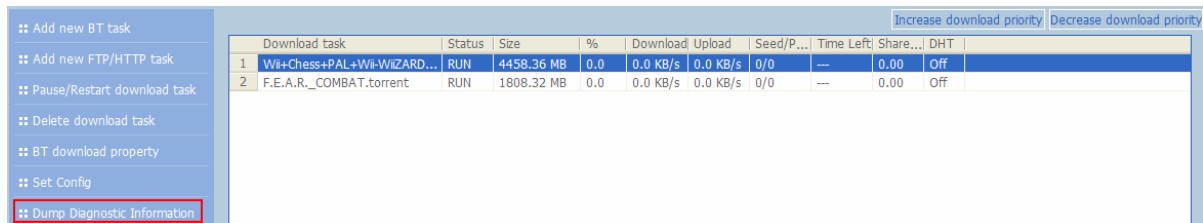


10. To logout Download Station, click  on the top right hand corner.
11. To access the folders you have downloaded, please go to the share folder **Qdownload** of the NAS.

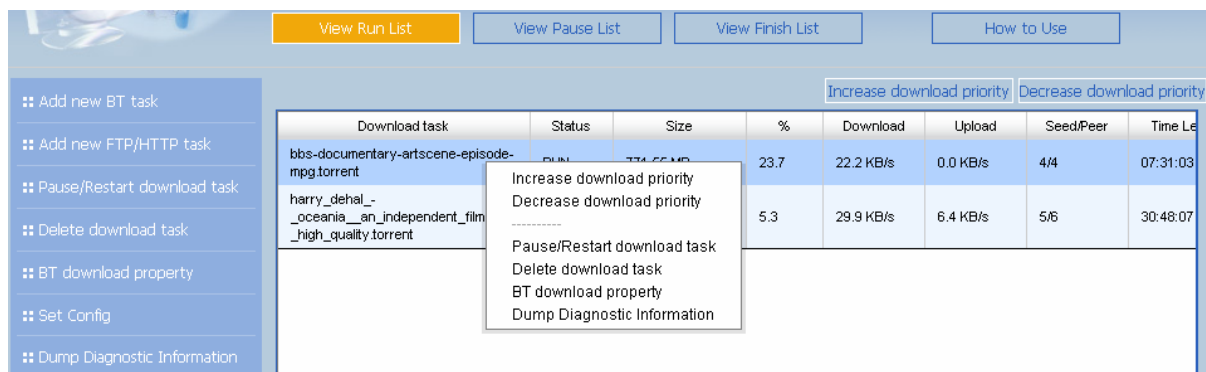


## Dump Diagnostic Information

To view the diagnostic details of a download task, select a task on the list and click "Dump Diagnostic Information".



You can right click the download task to configure the download settings.



The common reasons for slow BT download rate or download error are as follow:

1. The torrent file has expired, the peers have stopped sharing this file, or there is error in the file.
2. The NAS has configured to use fixed IP but DNS server is not configured, or DNS server fails.
3. Set the maximum number of simultaneous downloads as 3-5 for the best download rate.
4. The NAS is located behind NAT router. The port settings have led to slow BT download rate or no response. You may try the following means to solve the problem:
  - a. Open the BitTorrent port range on NAT router manually. Forward these ports to the LAN IP of the NAS.
  - b. The new NAS firmware supports UPnP NAT port forwarding. If your NAT router supports UPnP, enable this function on the NAT. Then enable UPnP NAT port forwarding of the NAS. The BT download rate should be enhanced.

## 6.1 Use Download Software QGet

QGet is a powerful management software for maintaining the BT, HTTP and FTP download tasks of multiple TS series NAS via LAN or WAN. By using QGet, you no longer need to login the Download Station web interface of multiple servers and manage the settings one by one. Simply install QGet on any computer running Windows 2000/XP/Mac, you can manage the download tasks of all your NAS servers.

1. To use QGet, install the software from the product CD-ROM.



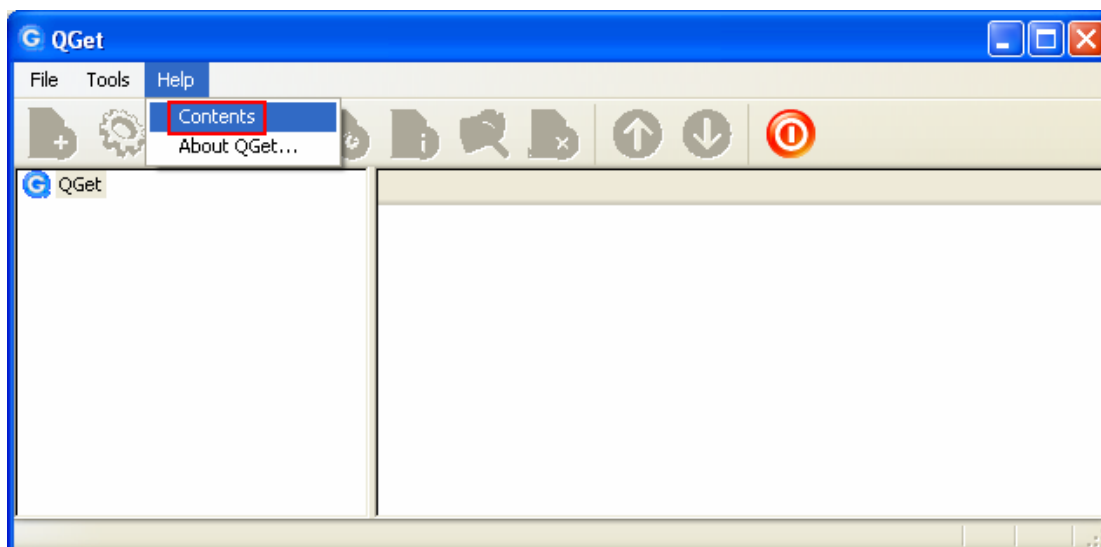
2. Follow the instructions to install QGet.



3. Run QGet from the installed location.



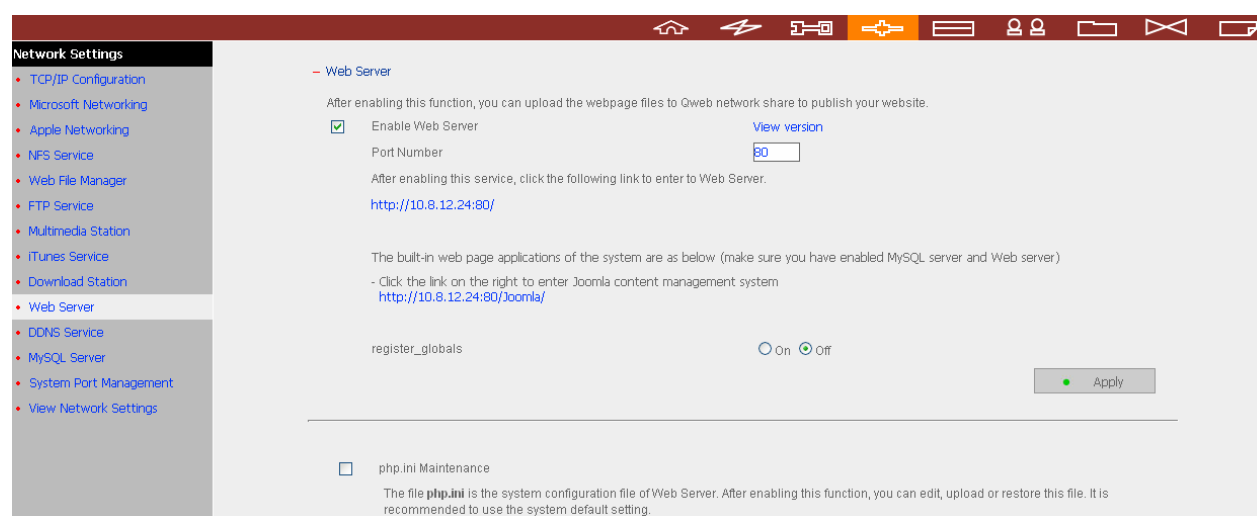
4. For the details of using QGet, please refer to the online help of the software.



## Chapter 7. Web Server

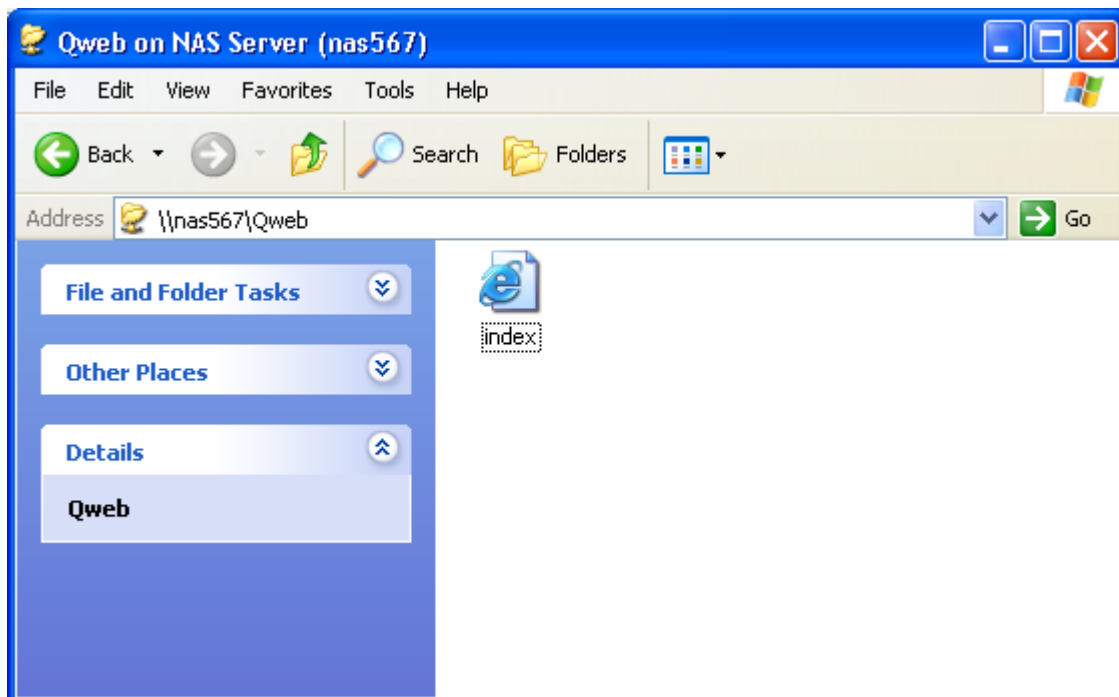
The NAS enables you to upload web pages and manage your own website easily by Web Server function. It supports Joomla!, PHP and SQLite for you to establish an interactive website.

1. To use Web Server, make sure a SATA disk is installed correctly in the NAS. A share folder **Qweb** is created. Enable Web Server function and enter the port number in **Network Settings**.



2. You can upload your web pages to the folder Qweb by the following methods:
  - a. By using samba: You can open a web browser and type **\\[NAS IP]\Qweb** or **\\[NAS name]\Qweb**. Login the folder and upload your web pages.
  - b. By FTP: You can login FTP service and upload your web pages to the folder (please refer to Chapter 8).
  - c. By Web File Manager: You can login Web File Manager and upload your web pages to the folder (please refer to Chapter 9).

The file index.html, index.htm, or index.php is the home path of your webpage.



3. Click the link <http://NAS IP:80/> on Web Server page or click "Web Server" on the login page of the NAS to access the web page you upload. Note that when Web Server is enabled, you have to enter [http://NAS IP address:8080] in your web browser to access the login page of the NAS.

**Web Server**

After enabling this function, you can upload the webpage files to Qweb network share to publish your website.

☒ Enable Web Server [View version](#)

Port Number

After enabling this service, click the following link to enter to Web Server.  
<http://10.8.12.24:80/>

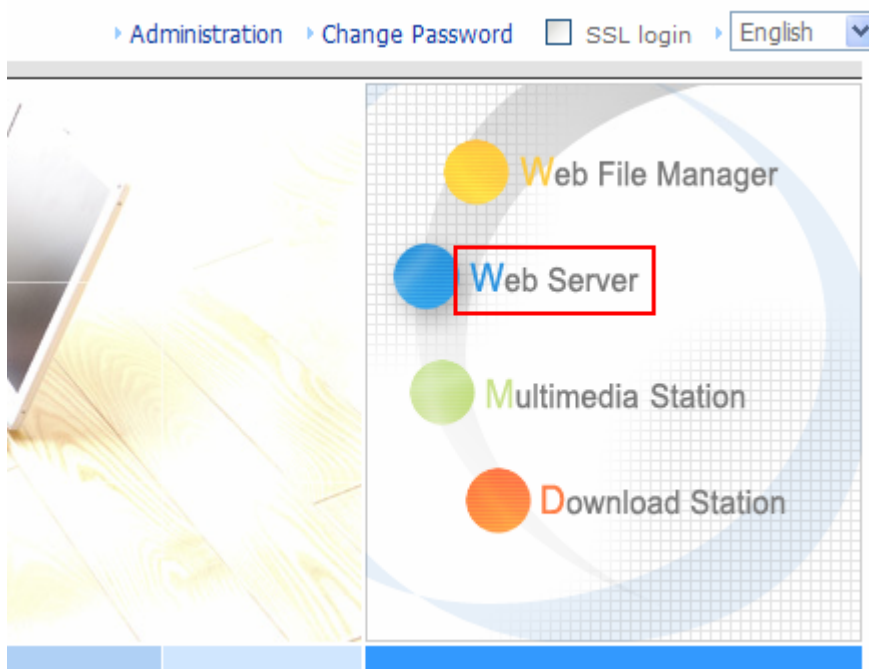
The built-in web page applications of the system are as below (make sure you have enabled MySQL server and Web server)  
- Click the link on the right to enter Joomla content management system  
<http://10.8.12.24:80/Joomla/>

register\_globals ☐ On ☒ Off

---

☐ php.ini Maintenance

The file **php.ini** is the system configuration file of Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended to use the system default setting.





## MySQL Management

The first time you install the system, the phpMyAdmin software is automatically installed as the MySQL management tool. When you update the firmware in the future, phpMyAdmin will not be re-installed and your data on the database will not be overwritten or changed.

The phpMyAdmin program files are created in the Qweb share folders. You can change the folder name and access the database by entering the URL in the browser. However, the link on the web management interface is not changed.



**Note:** The default user name of MySQL is "root". The password is "admin". Please change your root password immediately after logging in to the phpMyAdmin management interface.

## SQLite Management

SQLiteManager is a multilingual web-based tool to manage SQLite databases and can be downloaded from <http://www.sqlitemanager.org/>.

Please follow the steps below or refer to the INSTALL file in the downloaded SQLiteManager-\*.tar.gz<sup>?</sup> to install the SQLiteManager.

- (1) Unpack your download file SQLiteManager-\*.tar.gz.
- (2) Upload the unpacked folder **SQLiteManager-\*** to **\\NAS IP\Qweb\**.
- (3) Open your web browser and go to **http://NAS IP/SQLiteManager-\*/**.

<sup>?</sup>: The symbol "\*" refers to the version number of SQLiteManager.

## Chapter 8. FTP Server

The NAS supports FTP service. To use FTP service, enable this function in **Network Settings** and follow the steps below:

The screenshot shows the 'Network Settings' page with a sidebar on the left containing a list of settings: TCP/IP Configuration, Microsoft Networking, Apple Networking, NFS Service, Web File Manager, FTP Service (highlighted), Multimedia Station, iTunes Service, Download Station, Web Server, DDNS Service, MySQL Server, System Port Management, and View Network Settings. The main content area is titled 'FTP Service' and contains the following configuration options:

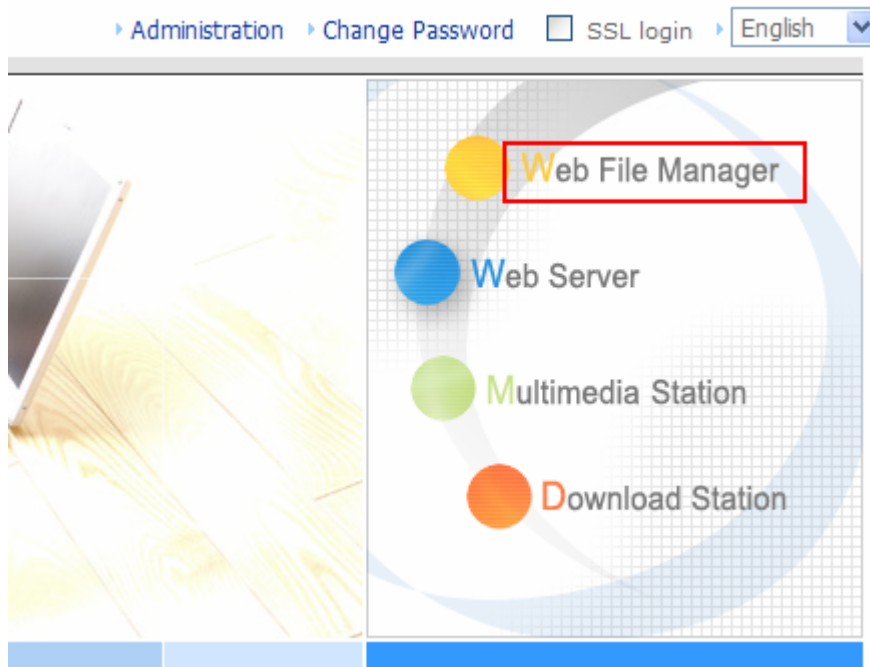
- ☒ Enable FTP Service
- Protocol type:
  - ☒ FTP (standard)
  - ☐ FTP with SSL/TLS (Explicit)
- Port Number:
- Unicode Support: ☐ Yes ☒ No
- Enable Anonymous: ☐ Yes ☒ No
- Passive FTP Port Range:
  - ☒ Use the default port range (55536 - 56559)
  - ☐ Define port range:  -
- ☐ Respond with external IP address for passive FTP connection request
- External IP address:
- Maximum number of all FTP connections:
- Maximum number of connections for a single account:
- ☐ Enable FTP transfer limitation (0 means unlimited)
  - Single connection: Maximum download rate (KB/s):  KB/s \* Maximum upload rate (KB/s):  KB/s

**Note:** If your FTP client does not support Unicode, please select "No" for Unicode Support and select a supported filename encoding from **[Filename Encoding Setting]** under [System Settings] so that the folders and files on FTP can be properly shown.







At the bottom right, there is an 'Apply' button with a green dot icon.

1. Open an IE browser and enter **ftp://[NAS IP]** or **ftp://[NAS name]**. OR

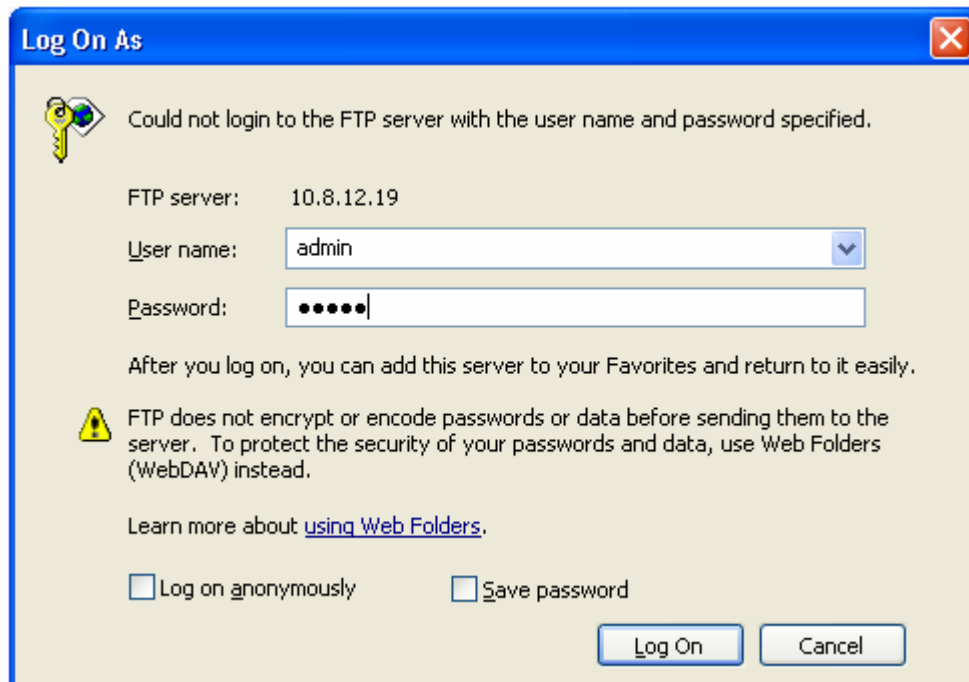
2. By Web File Manager of the NAS.
  - a. Go to the NAS administration page and click "Web File Manager". Enter user name and password to login the NAS.



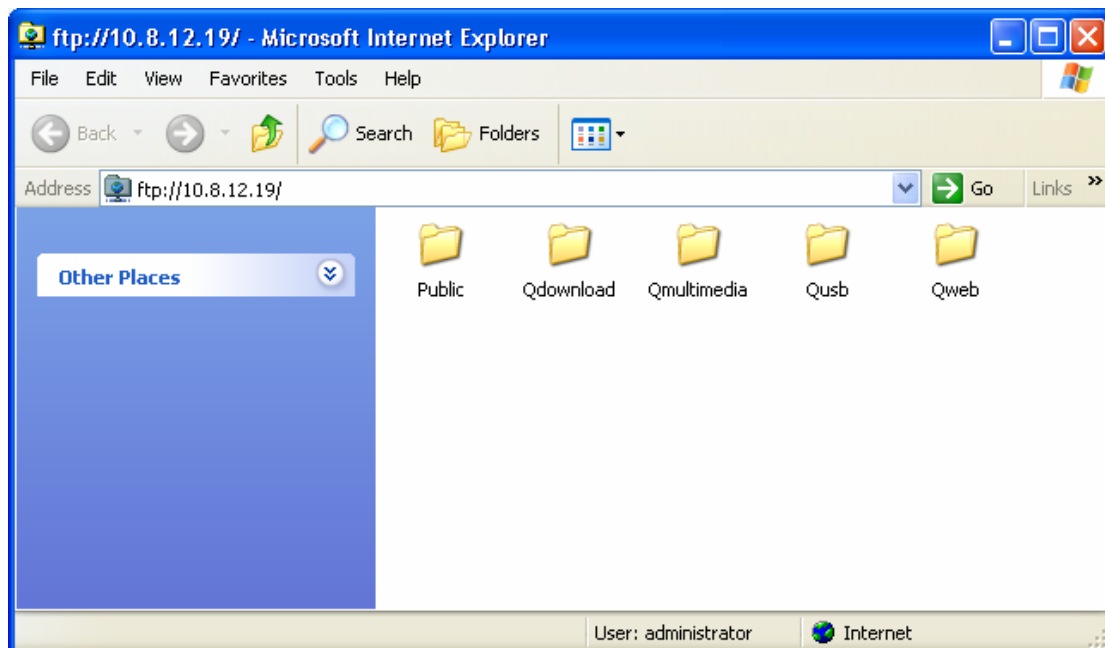
- b. Click "FTP".

FTP		
	Share Folder	Comment
	 Public	System default share
	 Qdownload	System default share
	 Qmultimedia	System default share
	 Qusb	System default share
	 Qweb	System default share

- c. Enter the user name and password to login FTP service.



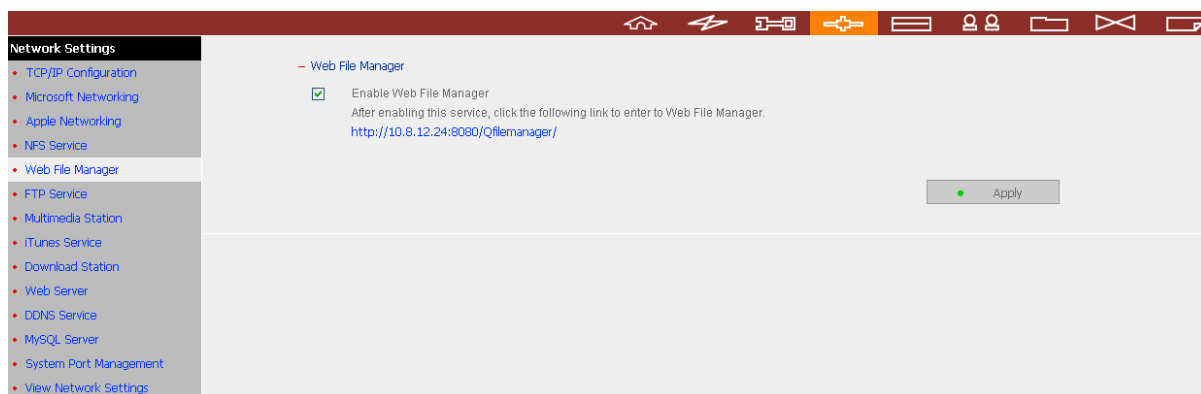
- d. You can start to use the FTP service.



# Chapter 9. Web File Manager

## Using Web File Manager

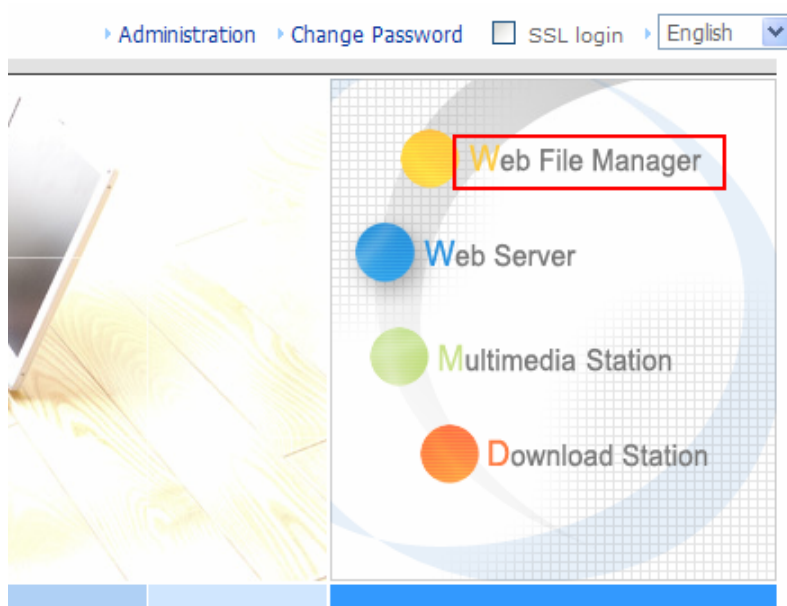
To use Web File Manager, enable this service in Network Settings.



Launch the web browser and go to the NAS administration page. Select **Web File Manager** and enter the correct login name and password. You can login as “guest” to access the network shares open to guest access on the NAS. The login password of guest is **guest**.



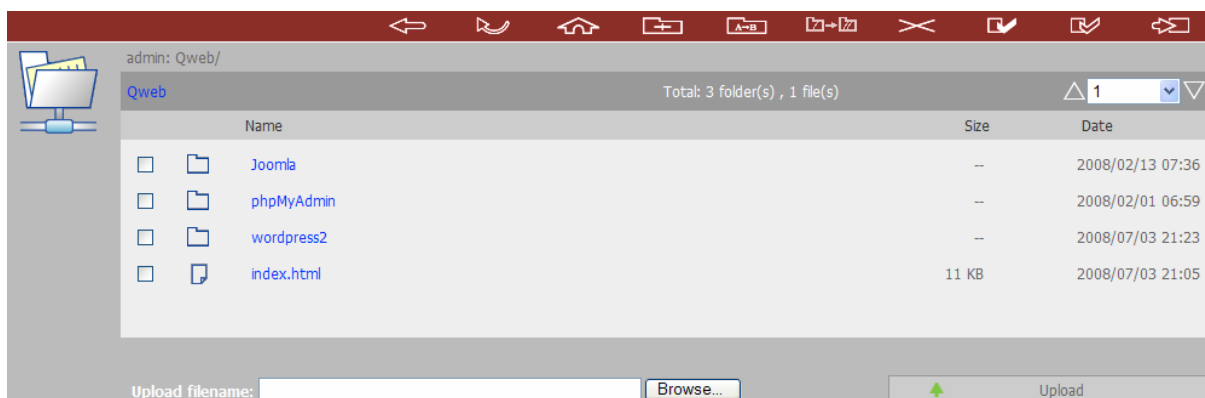
**Note:** Make sure a network share is created before using Web File Manager.



Select a network share.




You can organize share folders of the NAS. With Web File Manager, you can upload, rename, or delete files and folders in the network shares.




### View files online

Click a file displayed on the web page. The information of the file is shown. If your browser does not support the file format, a download window pops up automatically. Download the file and you can open it on your PC.


### Create folder

- Select a network share or folder in which you want to create a new folder.
- Click  (Create Folder) on the toolbar.
- Enter the name of the new folder and click "OK".


### Rename file or folder

- i. Select a file or folder to rename.
- ii. Click  (Rename) on the toolbar.
- iii. Enter the new file or folder name and click "OK".

### Move/copy files or folders

- i. Select the files or folders to move or copy.
- ii. On the tool bar, click  (Move/Copy).
- iii. You can select the destination folder to which the selected files or folders are moved or copied.

### Delete file or folder

- i. Select a file or folder to delete.
- ii. Click  (Delete) on the toolbar.
- iii. Confirm to delete the file or folder.

To delete all files and folders, click  (Select All) and  (Delete).


### Upload file

- i. Open the folder to upload file to.
- ii. Click "Browse" to select the file.
- iii. Click "Upload".

### Download file

- i. Select a file to download.
- ii. Right click the file and select "Save Target As" to save the file.

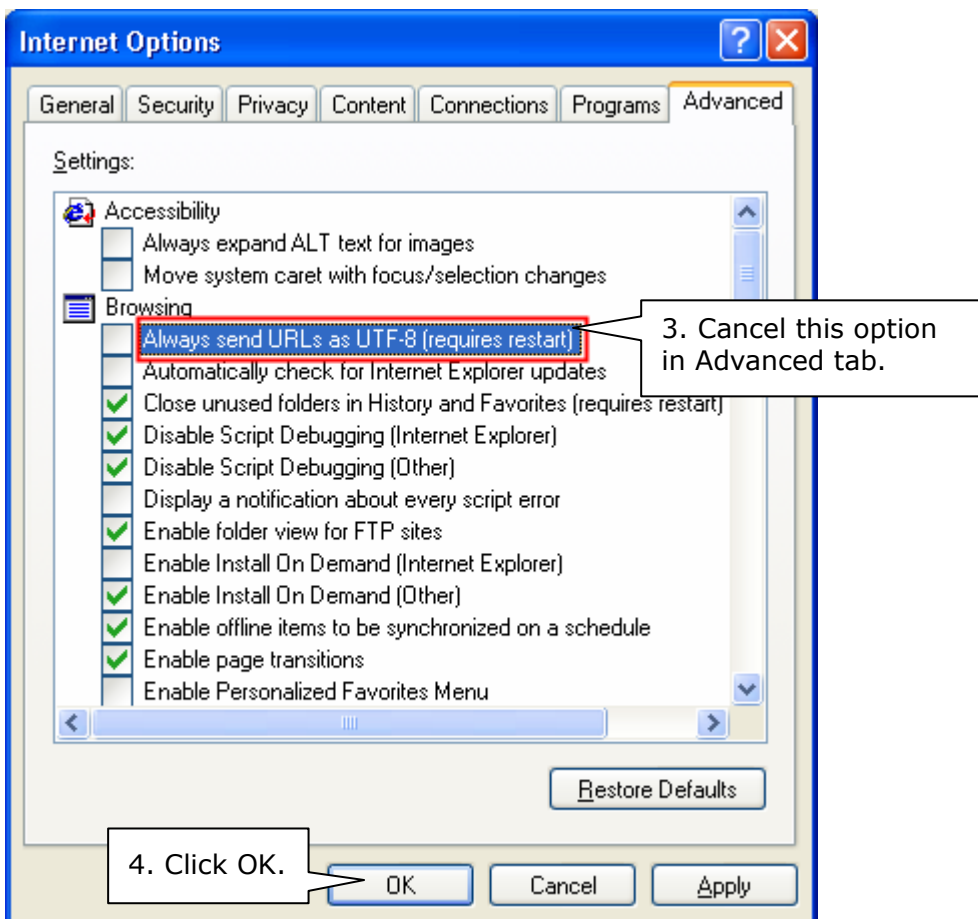
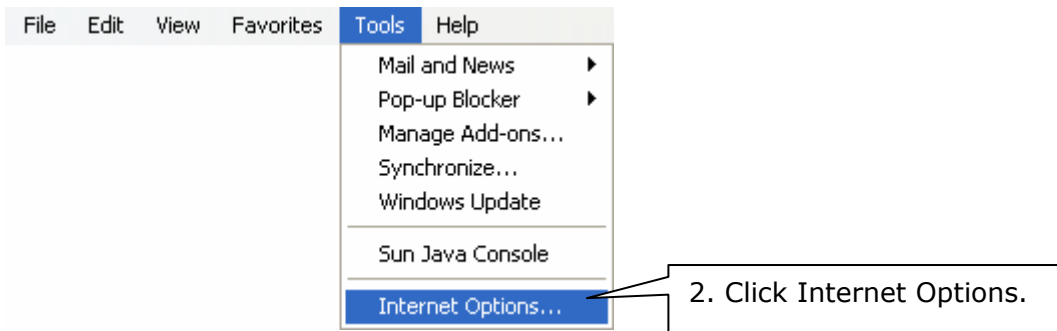
### Logout

To exit Web File Manager, click  (Logout).

## View Files Named in Local Language

To view files named in Chinese, you may have to configure the browser settings. Take Internet Explorer as an example, follow the steps below to configure the settings.














1. Click "Tools" in IE browser.



5. Restart the browser.



## Web File Manager Icons

Icon	Description
	Return to the parent folder
	Refresh the current page
	Return to network share list home page
	Create folder
	Rename file or folder
	Move/copy files or folders
	Delete file or folder
	Select all
	Cancel selection
	Logout
	Full access network share folder
	Read-only network share folder
	Malfunction network share folder

## Chapter 10. NetBak Replicator

NetBak Replicator is a powerful program installed in user's system (Windows® OS only) for data backup. You can back up any files or folders on local PC to specified share folder on the NAS by LAN or WAN.

### Main Functions

#### 1. Backup

- **Instant Backup**  
Select files and folders on local PC and back up files to specified network share folder on the NAS immediately.
- **File Filter**  
Select particular file types to be excluded from backup. The system filters all files belonging to these file types when backing up data.
- **Schedule**  
Specify a schedule for backing up data with this option, e.g. 12:00 every day or 05:00 every Saturday.
- **Monitor**  
When this option is enabled, the system uploads all files or folders to the server instantly for backup when the files or folders are modified.

#### 2. Restore

Select this option to restore backed up data to the original location of the file or to a new directory.

#### 3. Log

Enable this option to record events of NetBak Replicator, e.g. the time when NetBak Replicator starts and terminates.


## Install NetBak Replicator

1. Select **Install NetBak Replicator** in the NAS CD-ROM.



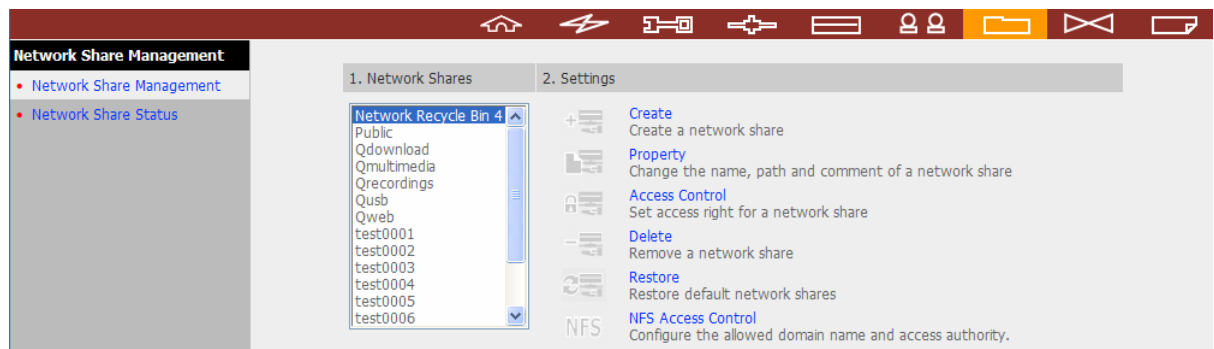
2. Follow the steps to install NetBak Replicator.




3. Upon successful installation, a shortcut icon  is shown on the Desktop. Double click the icon to run NetBak Replicator.

## Use NetBak Replicator

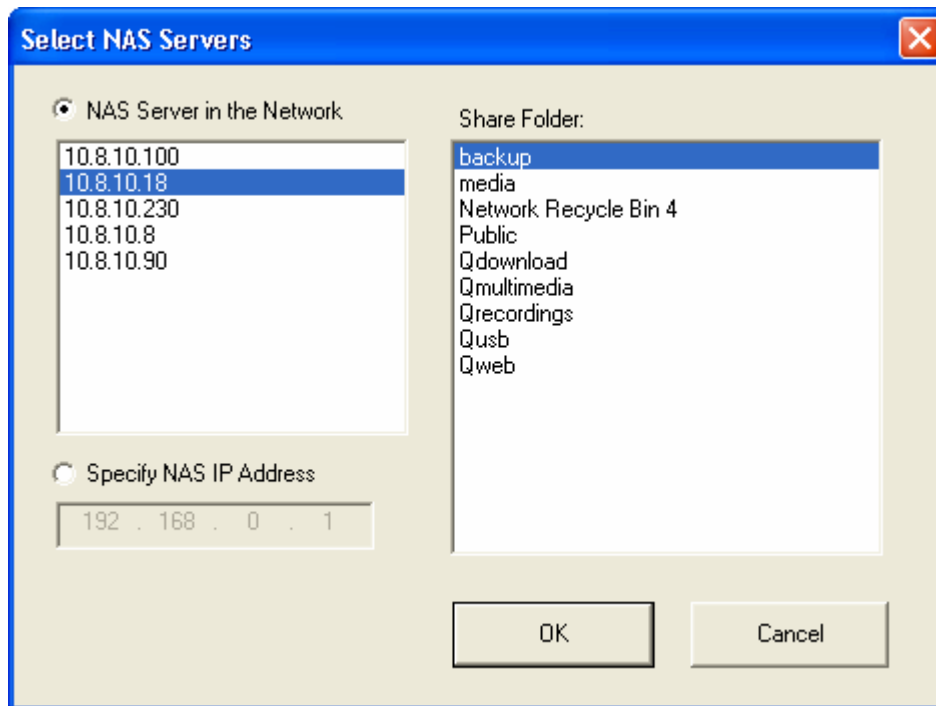
1. Before using NetBak Replicator, please login the NAS administration and go to **Network Share Management** to create a share folder for backup. Make sure the share folder is open for everyone access or you login the share folder with an authorized account or administrator by NetBak Replicator.



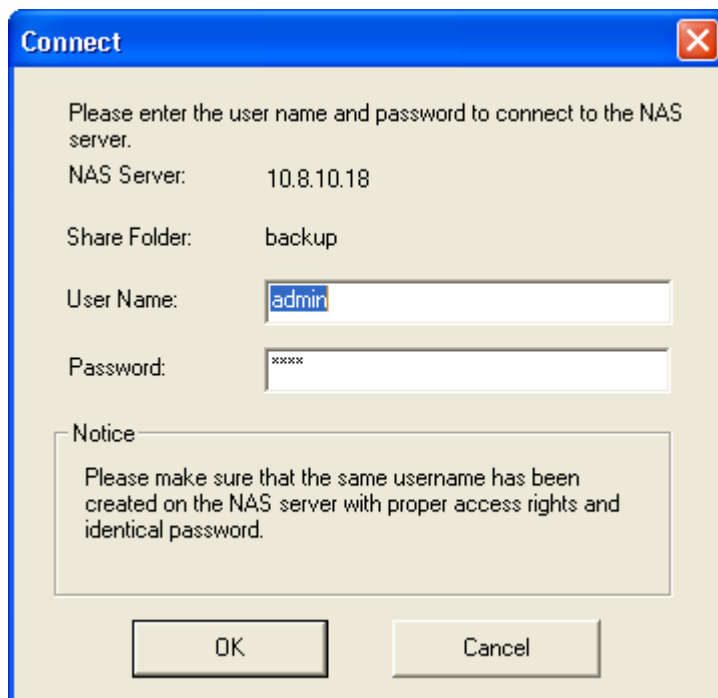
2. Run NetBak Replicator. Click . All the NAS and their share folders within the network are displayed.



- When the following window appears, all the NAS servers in the LAN appear on the left list. Select a server and a share folder on the right. NetBak Replicator also supports backup over WAN, you can enter the IP address of the NAS for data backup directly and select a share folder. Then click "OK".










- Enter the user name and password to login the server.



- You can start the backup procedure upon successful connection to the NAS.

## Description of Buttons on NetBak Replicator

	Open Configuration: Open a previously saved NetBak Replicator configuration.
	Save Configuration: Save the settings on NetBak Replicator. The file is named as *.rpr
	Select All: Select all items in the window.
	Clear All: Clear selection.
	Select My Document: Select all folders in My Document.
	Open NAS Backup Folder: This button allows users to find out where the files were backed up, and check or manage the archived files manually.
	Advanced Backup: Advanced Backup allows power user to back up a single folder with more advanced options.

- **Backup**

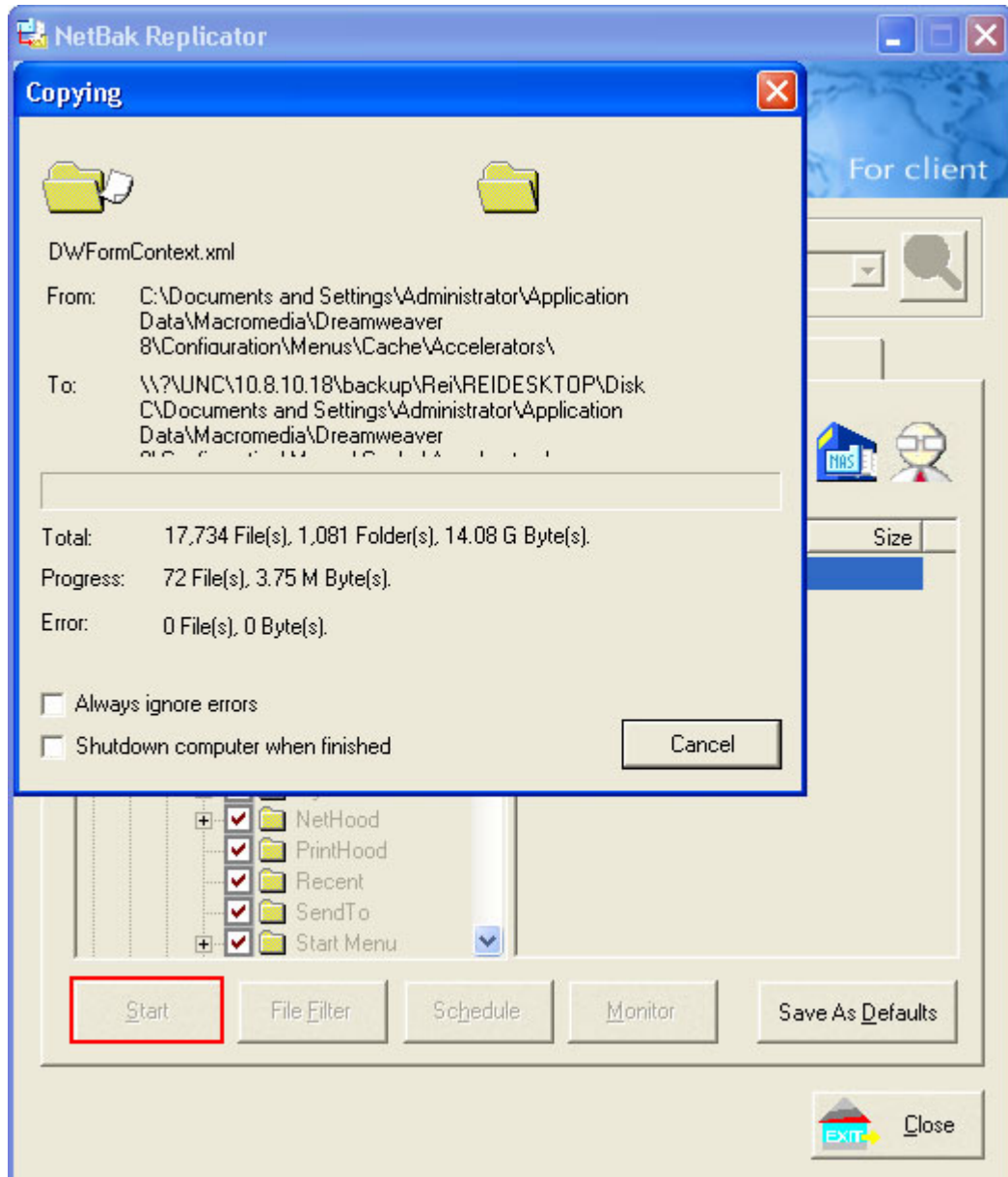
Select files and folders for backup.





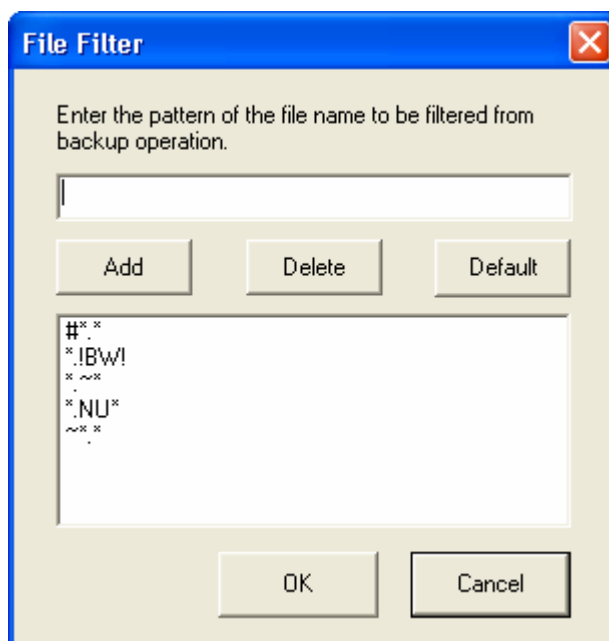
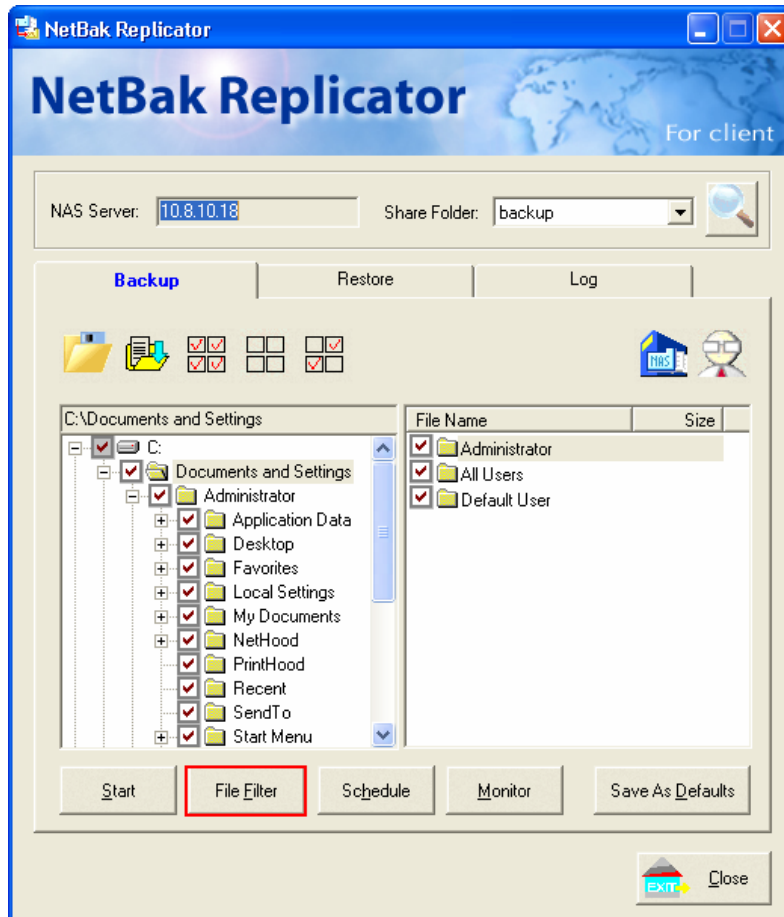
✓ Start

When you have selected the files for backup to the NAS, click "Start". The program starts to copy the selected files to the specified share folder on the NAS.



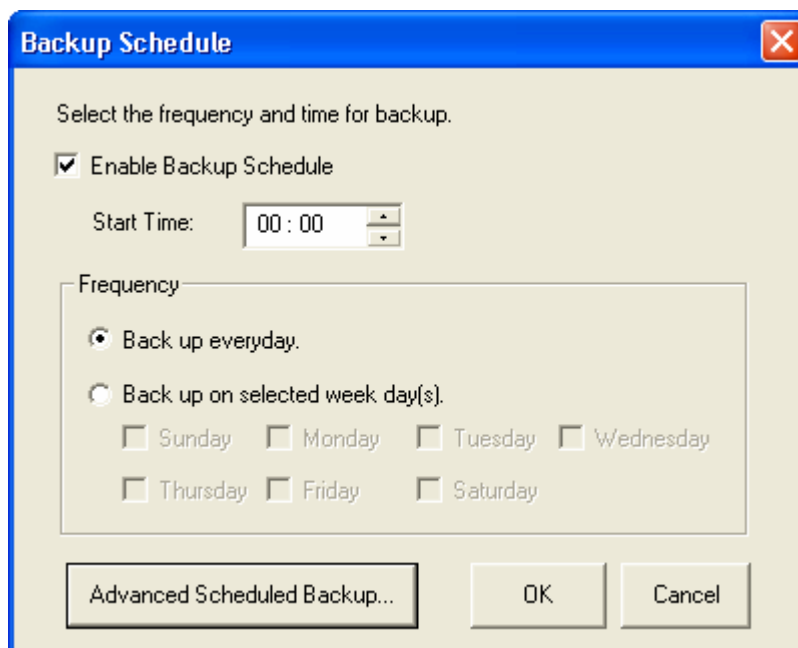
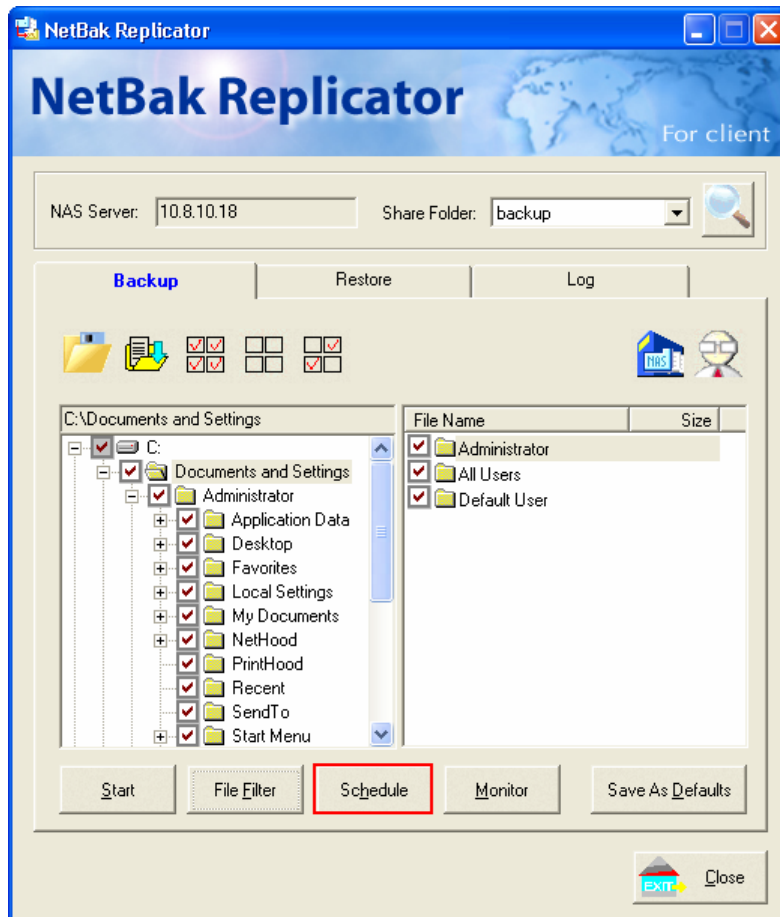
✓ File Filter

Click "File Filter" to select file format to be skipped from backup. Then click "OK".




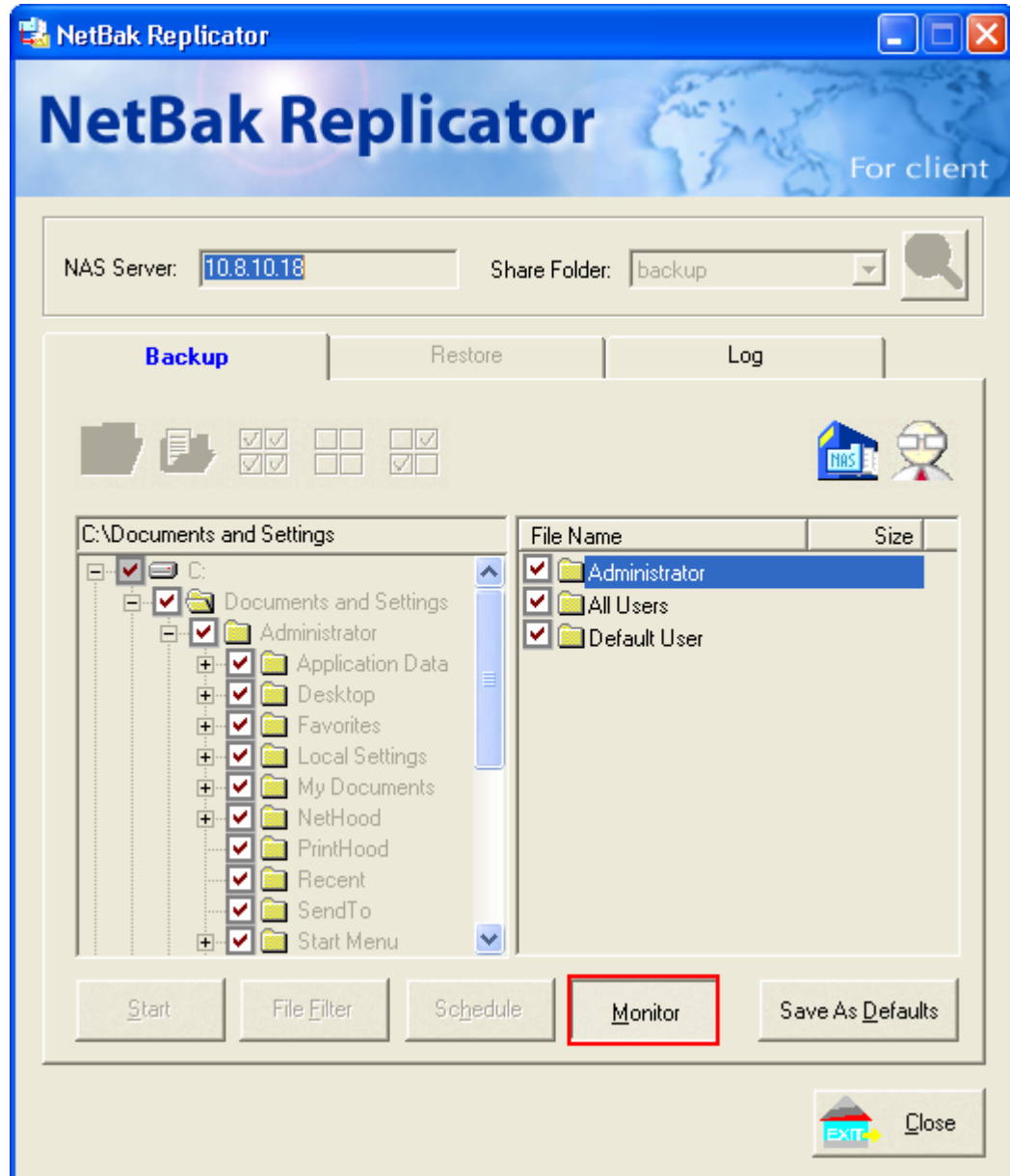
✓ Schedule

Click "Schedule". Then check the box "Enable Backup Schedule" and select the frequency and time for backup. Click "OK" to confirm.



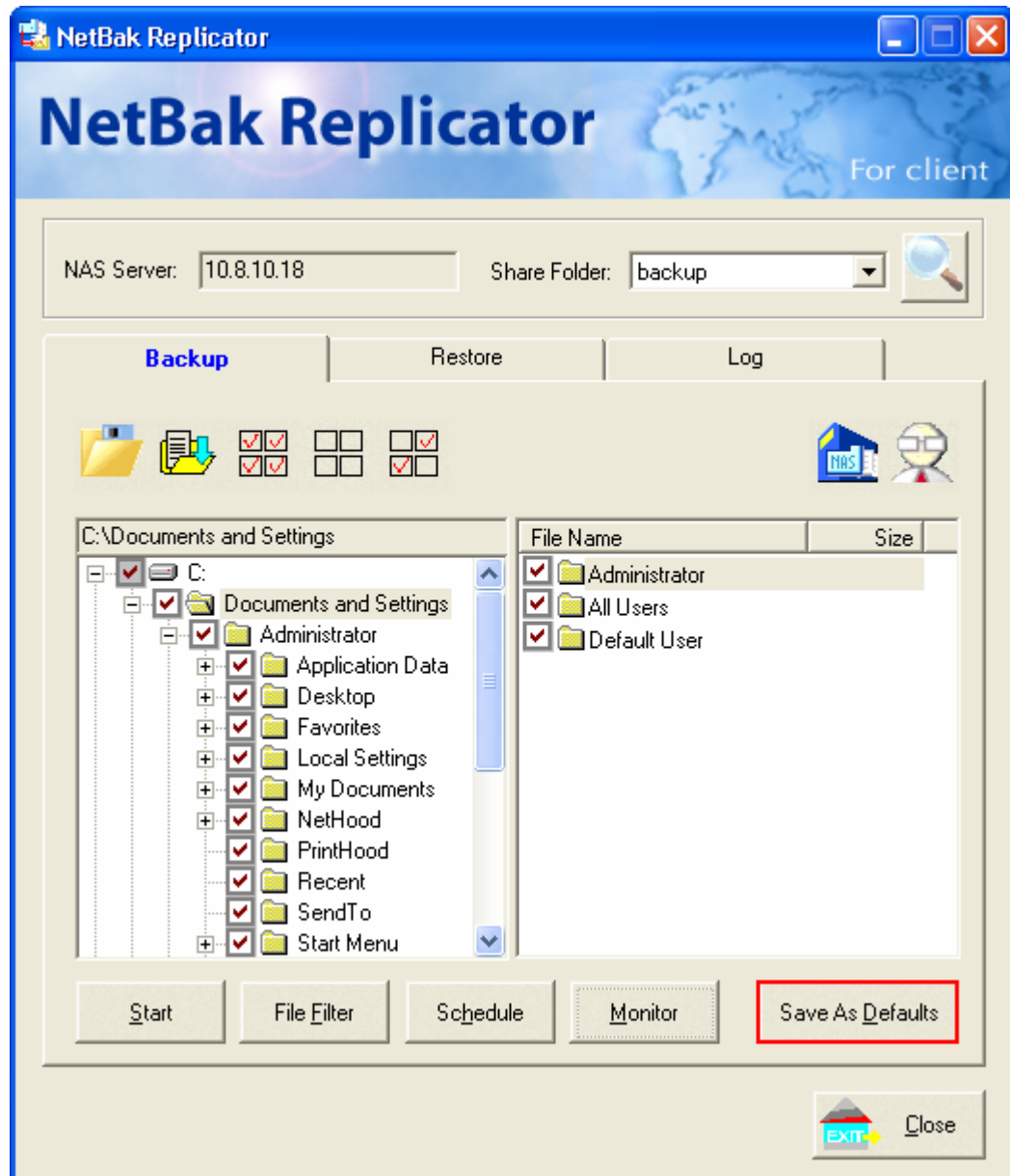
✓ Monitor

Select a folder for monitoring. When this option is enabled, the files or folders are copied to the NAS instantly when they are modified. Other files are gray and cannot be selected. Click "Monitor" again to enable or disable monitoring. An icon  appears on the task bar of Windows® when monitoring is in process.




✓ Save as Defaults

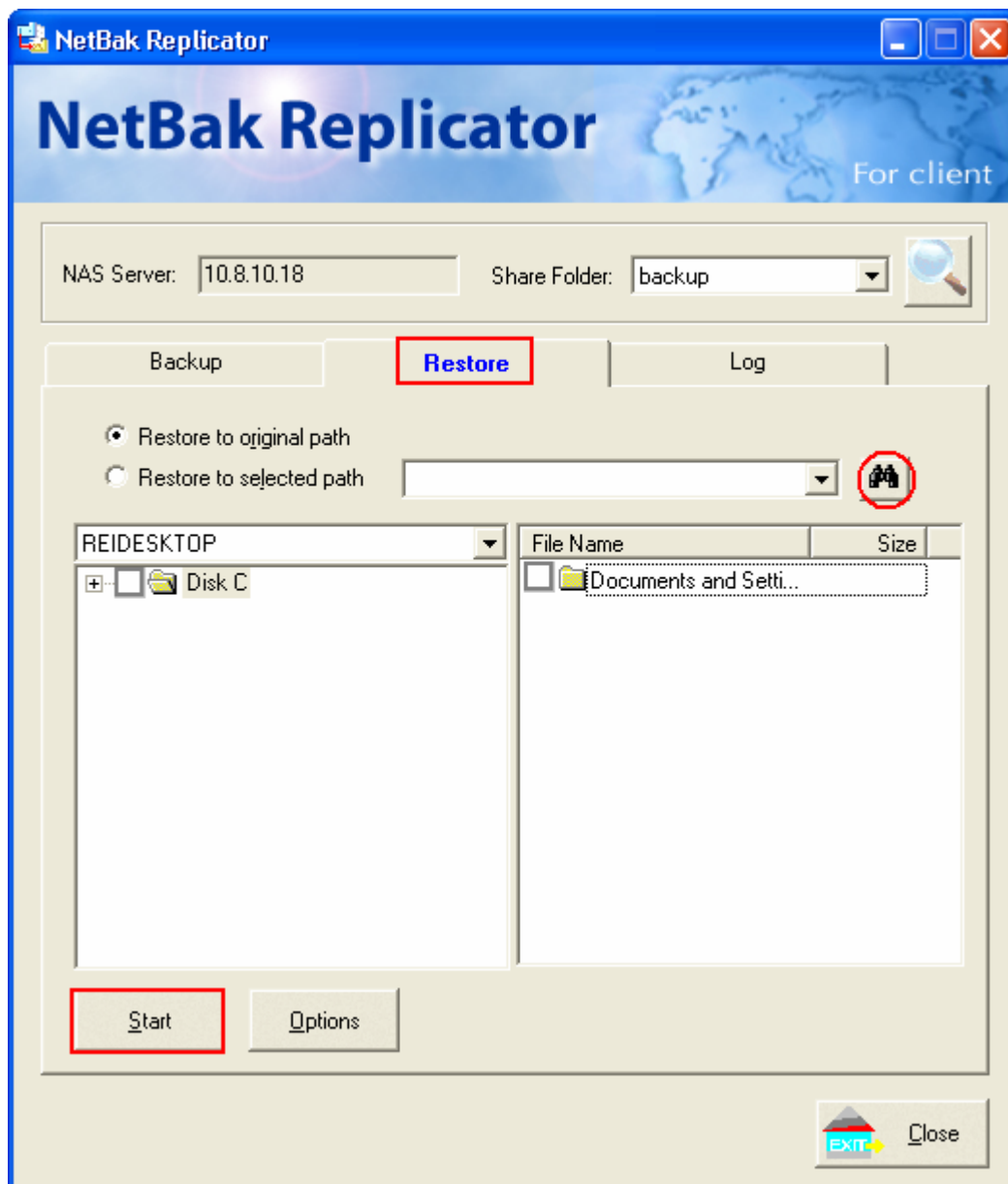
when using this function, NetBak Replicator records all current settings of the user, including whether or not monitor function is enabled. When the user login again, this program loads the previous recorded settings for users to manage data backup.



- **Restore**

Please follow the steps below to restore files from the NAS to your PC.

- a. Restore to original position: Select the location that the data is restored to.
- b. Select new restore position: Click  to select the directory to restore data to or select a previously chosen location from the drop-down menu.
- c. Select the folder(s) and sub-folder(s) for restoring data on the right list and click "Start".



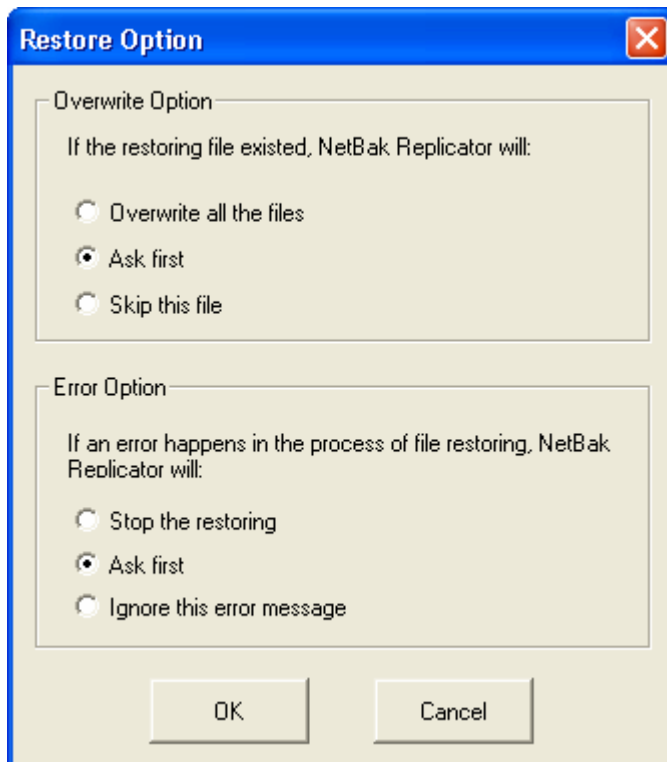
d. Option: Select recovery option and error option.

If the restoring file existed, NetBak Replicator will:

- ✓ Overwrite all the files
- ✓ Ask first
- ✓ Skip this file

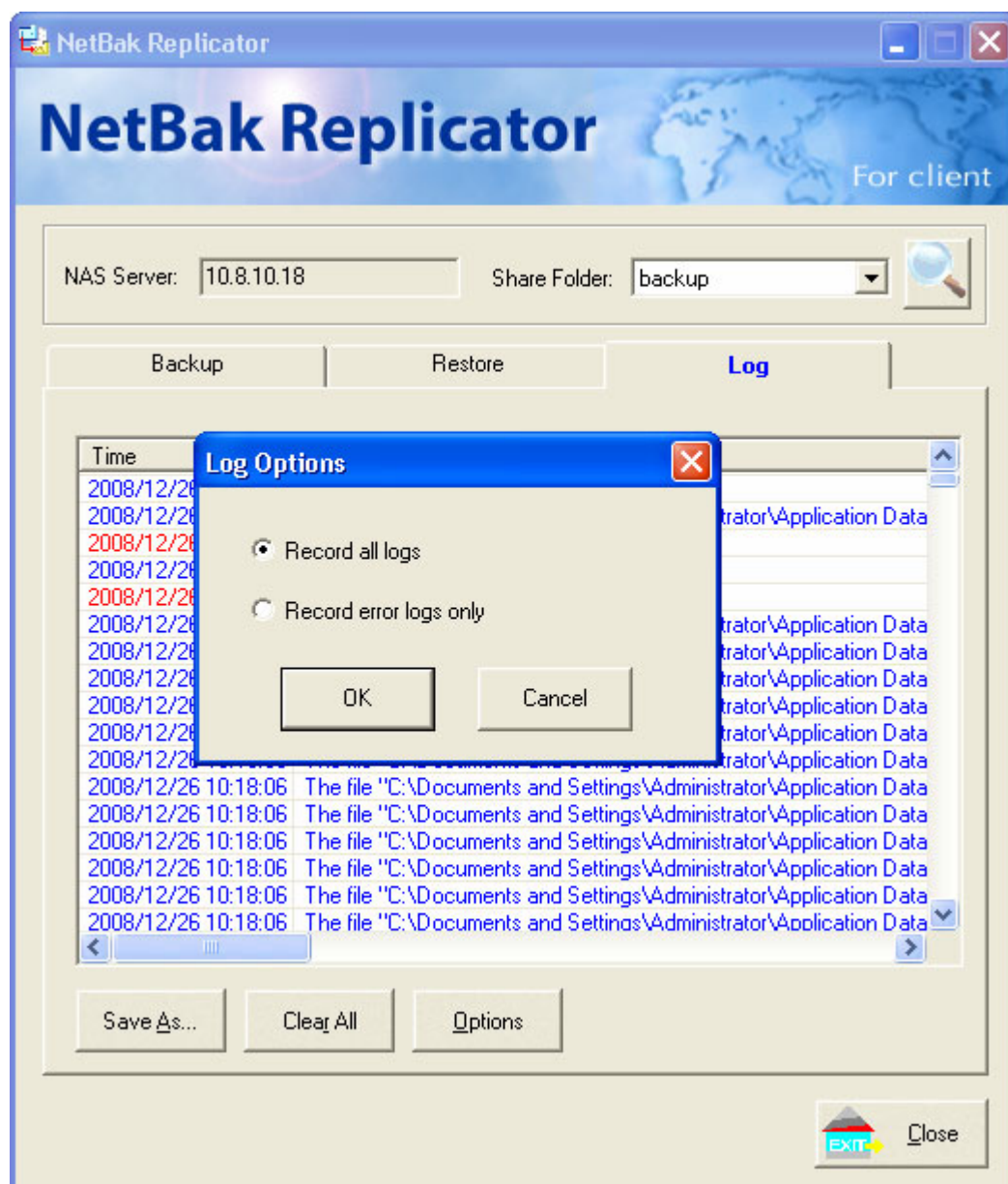
If an error happens in the process of file restoring, NetBak Replicator will:

- ✓ Stop the restoring
- ✓ Ask first
- ✓ Ignore this error message



- **Log**

- a. Save As...: To save all logs on NetBak Replicator, click this button. All logs are saved as text file.
- b. Clear All: Click this button to clear all logs.
- c. Option: Select the type of logs to be recorded— "Record all logs" or "Record error logs only".

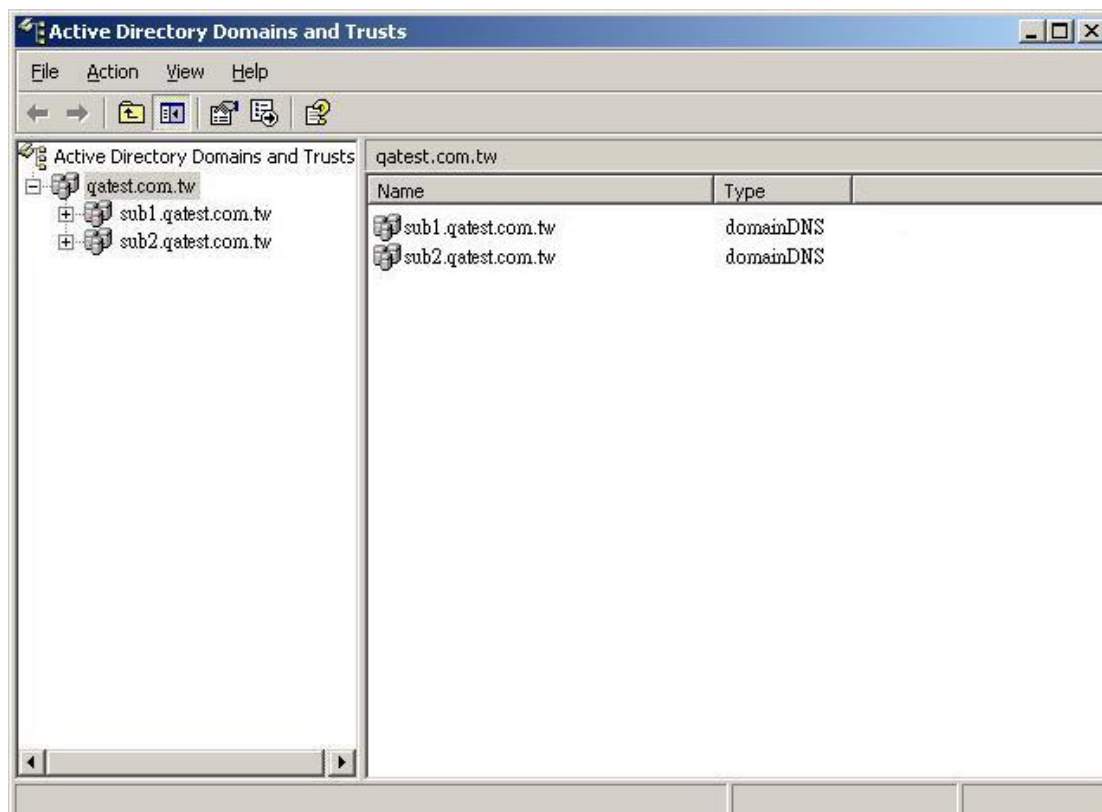




## Chapter 11. Configuring AD Authentication

The NAS supports Active Directory (AD). You can import the user accounts from Windows AD domain to the NAS. This saves your time to create users one by one. The example below demonstrates how to use this service.

We have two domains qatest.com.tw and sub2.qatest.com.tw controlled by Windows 2003 server, and a domain sub1.qatest.com.tw controlled by Windows 2000 server.



Please make sure you have enabled the Active Directory service on the Windows server and check the following items:

- The DNS server setting of the NAS must be assigned to AD server.
- The NAS and AD server can synchronize only if their time difference is less than 5 minutes.
- The NAS and AD server synchronize every 5 minutes. To configure the settings manually, the NAS has to be set as standalone mode and then added to AD domain.
- After adding to AD domain, you must login as Domain\_name\Username to access Network Neighborhood. Local users of the NAS cannot access the server by Network Neighborhood.
- It is suggested to use Windows 2000 Service Pack 4, or Windows 2003 Service Pack 1.
- When the NAS is added to AD domain, the authority of "everyone" does not work, "everyone" is the default account of the NAS, but is not supported in AD domain. Therefore the authority has to be reset.
- The IP address of the AD server should be recorded in the DNS settings on the AD server.
- You must change the password of "administrator" after you create "Active Directory" service on the AD server.
- The DNS server on the AD Server should have two records on it. For example, when the AD server name is 2003tc.testad.com, the records will be:

2003tc.testad.com	A	192.168.1.100
-------------------	---	---------------

Testad.com	A	192.168.1.100
------------	---	---------------

One is "A record" for AD server, and the other is the domain "A record" for DNS queries.

## Adding the NAS to Windows Server 2003 Active Directory Domain

1. In TCP/IP Configuration in Network Settings, enter the IP address of Windows AD server as the primary DNS Server IP.

**TCP/IP Configuration**

Configuration of Network Interfaces ☒ Failover ☐ Load balancing ☐ Standalone

**Failover**

Network transfer rate: Auto-negotiation

☐ Obtain IP address settings automatically via DHCP

☒ Use static IP address

Fixed IP Address: 172 . 17 . 21 . 123

Subnet Mask: 255 . 255 . 254 . 0

Default Gateway: 172 . 17 . 20 . 1

Primary DNS Server: 172 . 17 . 22 . 208

Secondary DNS Server: 0 . 0 . 0 . 0

2. Go to Microsoft Networking of Network Settings. Enable AD Domain Member, and enter the domain name and the user name with administrator access right to that domain.

**Microsoft Networking**

☒ Enable file service for Microsoft networking

☐ Standalone Server

☒ AD Domain Member

Server Description: NAS Server

Workgroup: QNAP

AD Server Name: ad2008

Domain Name: qnap.com

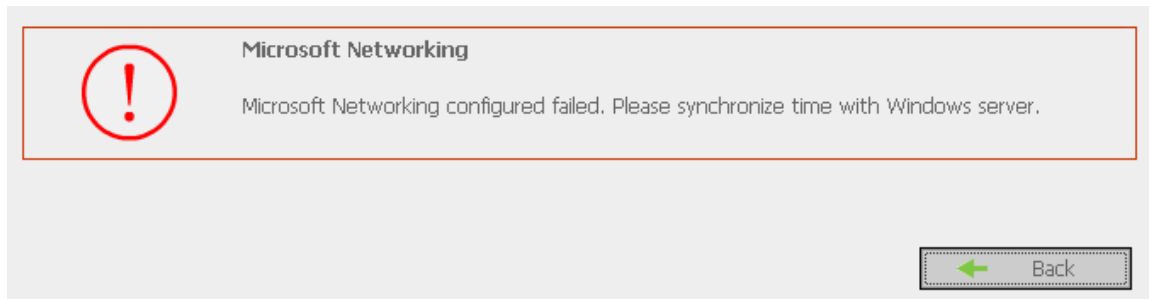
Domain Username: qnaptest

Password: ....

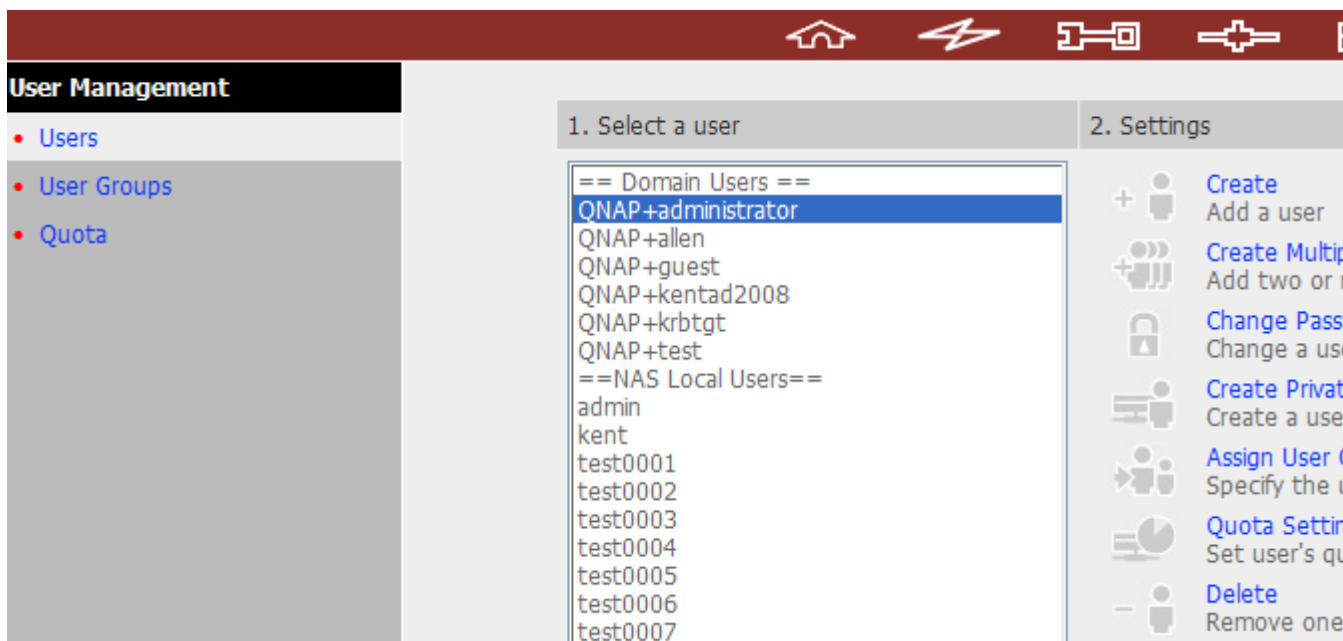
### Note:

- a. Make sure that a fully qualified domain name such as qnap.com is filled in.
- b. The user name must have administrator access right to that domain.

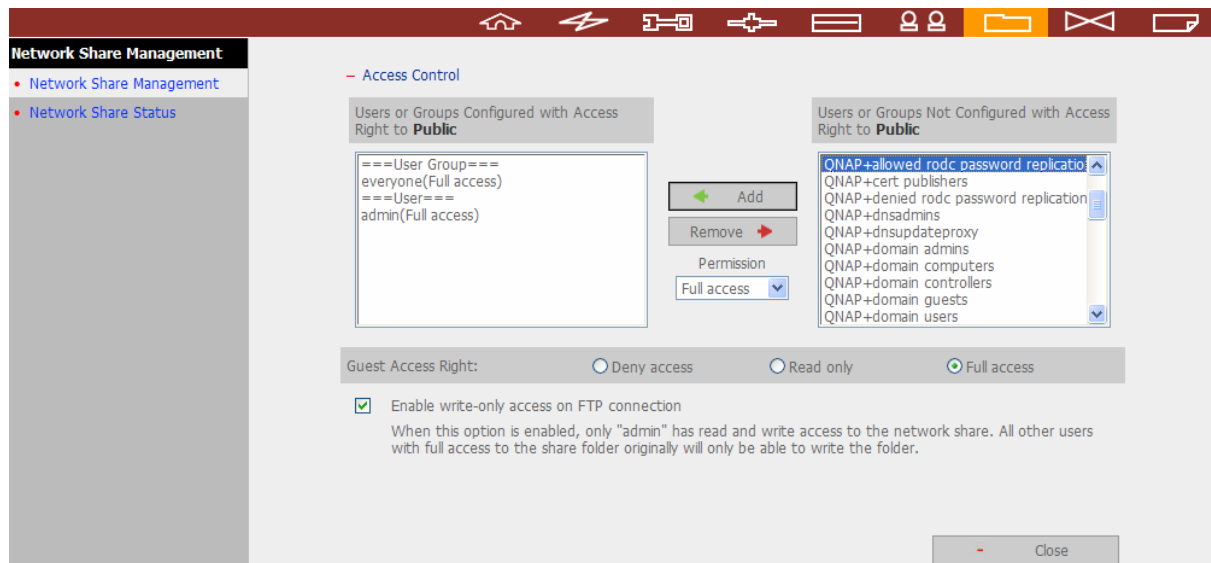
- When the following message appears after applying the settings in step 2, check the time zone settings. Make sure the difference of your time and that of AD server is less than 5 minutes. If the time difference is larger than 5 minutes, you will not be able to add the domain member.



- Upon successful adding of domain member, you can view the list of domain users and local users in User Management.

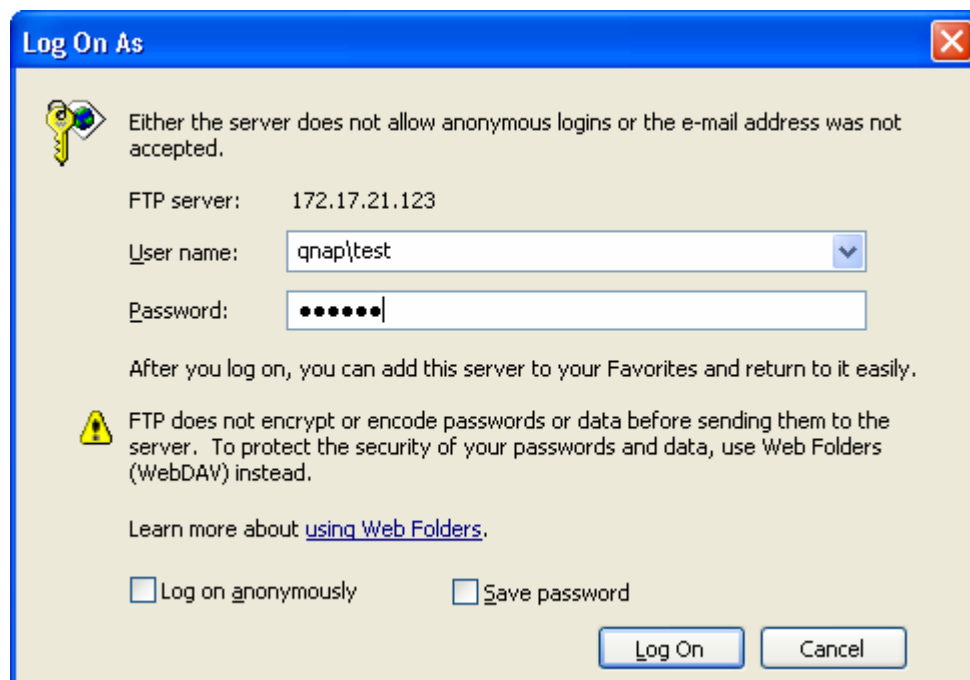


5. Go to "Access Control" in Network Share Management to configure the access control right of AD users to the NAS shares.



## Using AD users to access services

To access services like FTP, Network Neighborhood, or Apple Talk with an AD user account, add **DomainName\** in front of the user name when logging in.



## Chapter 12. Access the NAS from Linux

You can access the NAS from Linux by the steps below:

1. In Linux, run the following command:

**mount -t nfs <NAS IP address>:/<Network Share Name> <Directory to Mount>**

For example, if the IP address of your NAS is 192.168.0.1 and you want to link the network share folder "public" under the /mnt/pub directory, use the following command:

**mount -t nfs 192.168.0.1:/public /mnt/pub**

**Note:** You must login as "root" user to initiate the above command.

2. Login as the user ID you define, you can use the mounted directory to access your network share files.

## Chapter 13. NAS Maintenance

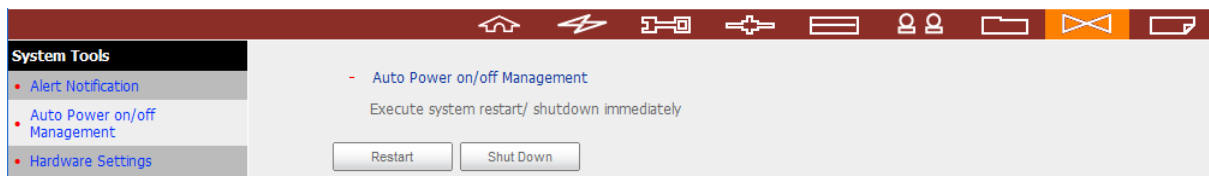
This section provides a general overview on system maintenance.

### 13.1 Restart/ Shut down Server

Follow the steps below to restart or shut down the NAS.

1. Login the administration page and go to "System Tools" > "Auto Power on/off Management".
2. Click "Restart" to reboot the server or "Shut Down" to turn off the server.

To force shut down the NAS server, press the power button for more than 10 seconds. After a long beep, the NAS shuts down immediately.



## 13.2 Reset Administrator Password and Network Settings

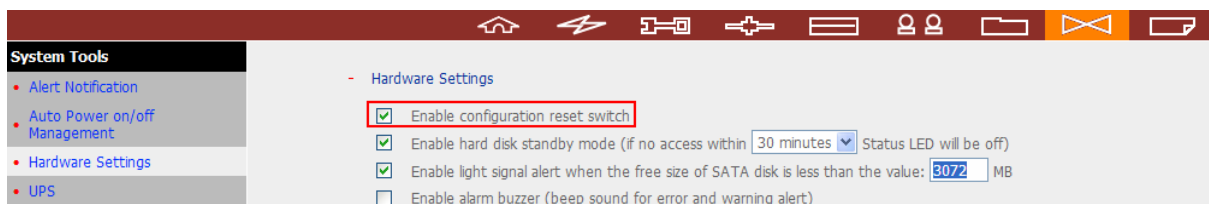
To reset the administrator password and network settings of the NAS, press the reset button of the NAS for a few seconds. A beep sound will be heard. The following settings are reset to default:

- System admin password: admin
- Network Settings/ TCP/IP Configuration: Obtain IP address settings automatically via DHCP
- Network Settings/ TCP/IP Configuration: Disable Jumbo Frame
- Network Setting/ System Port Management: 8080 (system service port)
- System Tools/ IP Filter: Allow all connections
- LCD panel password: (blank)

After the reset, you can login the NAS with the default user name and password:

Default user name: <b>admin</b> Password: <b>admin</b>
---

<b>Note:</b> To reset the system by the reset button, the option "Enable configuration reset switch" in Hardware Settings must be activated.
--





### 13.3 Disk Failure or Malfunction

When you encounter disk malfunction or failure, please do the following:

1. Record the malfunction status or error messages shown in Event Logs.
2. Stop using the failed NAS and turn off the server.
3. Contact your dealer or technical support.



**Note:** The NAS must be repaired by professional technicians, do not try to repair the server yourself.

Please back up any important files or folders to avoid potential data loss due to disk crash.

### 13.4 Power Outage or Abnormal Shutdown

In case of power outage or improper shutdown of the NAS, the system will resume to the state before it is shut down. If your server does not function properly after restart, please do the following:

1. If the system configuration is lost, configure the system again.
2. If the server does not function properly, contact your dealer or technical support.

To avoid the above situations, please back up your data periodically and make sure you have done the following:

- Follow the instructions described in Chapter 13.1 to restart or shut down the server.
- If there is an anticipated power outage, back up all important data and turn off the server properly until the power supply is resumed.

### 13.5 Abnormal Operation of System Software

When the system software does not operate properly, the NAS automatically restarts to resume normal operation. If you find the system restarts continuously, it may fail to resume normal operation. In this case, please contact the technical support immediately.

### 13.6 System Temperature Protection

When the system temperature exceeds 70°C (158°F), the system shuts down automatically for hardware protection.

## Chapter 14. RAID Abnormal Operation

### Troubleshooting

If the RAID configuration of your NAS is found abnormal or there are error messages, please try the following solutions:



**Note:** You must back up the important data on the NAS first to avoid any potential data loss.

1. Check that the RAID rebuilding has failed:
  - a. LED: The Status LED of NAS flashes in red.
  - b. In **Device Configuration/ SATA Disk** page, the status of the disk volume configuration is "In degraded mode".
2. Find out the hard drive(s) that causes the RAID rebuilding failure.
  - a. You can go to System Logs/ System Event Logs to search for the following error message and find out which hard drive(s) causes the error.

Error occurred while accessing Drive **X**.

Drive **X** has been removed.

**X** refers to the number of the hard drive slot.

#### 3. Troubleshooting

After plugging in the new hard drive (e.g., HDD 1), drive rebuilding will start. If the drive configuration fails again due to read/write error of the hard drive in the rebuilding process, identify which hard drive causes the error and follow the steps below to solve the problems.

**Situation 1:** The error is caused by the newly plugged in drive.

If the newly inserted drive (e.g., HDD 1) causes the rebuilding error, please unplug HDD 1 and plug in another new drive to start RAID rebuilding.

**Situation 2:** The error is caused by an existing drive (e.g., HDD 2) in the RAID configuration.

If the RAID configuration is RAID 1, you can do either one of the following:

- a. Back up the drive data to another storage device. Then reinstall and set up the NAS.
- b. Format the newly plugged in drive (e.g. HDD 1) as a single drive. Then back up the data on the NAS to this drive (HDD 1) via Web File Manager. Unplug the drive with errors (e.g., HDD 2). After that, insert a new drive to NAS to replace the fault drive, and execute RAID 1 migration.

**When the RAID configuration is RAID 5 or 6:** The RAID configuration is changed to degraded mode (read-only). It is recommended that you back up the data and run system installation and configuration again.

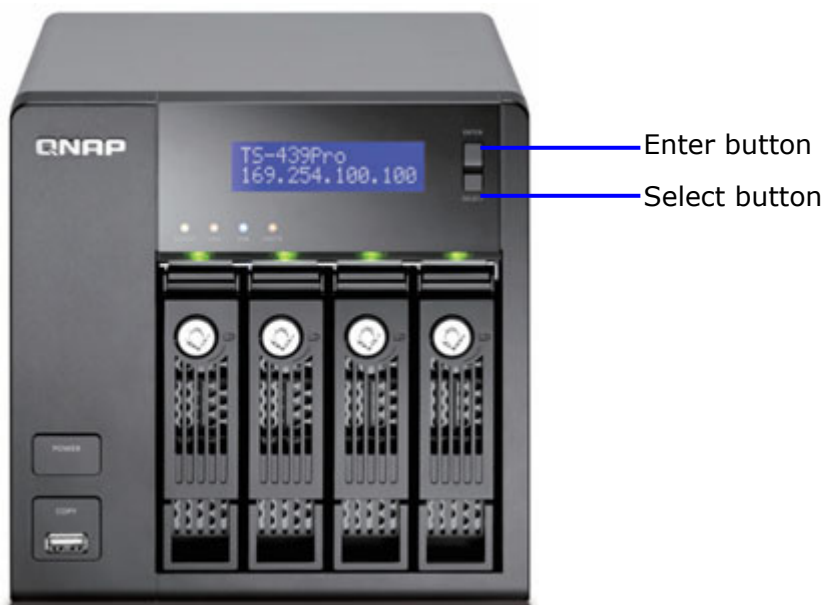


**Note:** When plugging in or unplugging a hard drive, please strictly adhere to the following rules to avoid abnormal system operation or data crash.

1. Plug in only one drive to NAS or unplug only one drive from NAS at one time.
2. After plugging in or unplugging a hard drive, wait for about ten seconds or longer until you hear two beeps from the NAS. Then unplug or plug in the next hard drive.

## Appendix A Use the LCD Panel

The NAS provides a handy LCD panel for you to perform disk configuration and view the system information.



When the NAS is started up, you will be able to view the server name and IP address:

N	A	S	5	F	4	D	E	3							
1	6	9	.	2	5	4	.	1	0	0	.	1	0	0	

For the first time installation, the LCD panel shows the number of hard drives detected and the IP address. You may select to configure the hard drives.

Number of hard drives detected	Default disk configuration	Available disk configuration options*
1	Single	Single
2	RAID 1	Single -> JBOD -> RAID 0 -> RAID 1
3	RAID 5	Single -> JBOD -> RAID 0 -> RAID 5
4	RAID 5	Single -> JBOD -> RAID 0 -> RAID 5 -> RAID 6

\*Press the "Select" button to choose the option, and press the "Enter" button to confirm.

For example, when you turn on the NAS with 5 hard drives installed, the LCD panel shows:

C	o	n	f	i	g	.		D	i	s	k	s	?		
<input type="checkbox"/>	R	A	I	D	5										

You can press the "Select" button to browse more options, e.g. RAID 6.

Press the "Enter" button and the following message shows. Press the "Select" button to select "Yes" to confirm.

C	h	o	o	s	e		R	A	I	D	5	?			
<input type="checkbox"/>	Y	e	s			N	o								

To encrypt the disk volume, select "Yes" when the LCD panel shows <Encrypt Volume?>.

The default encryption password is "admin". To change the password, please login the web-based administration interface as an administrator and change the settings in "Device Configuration" > "Disk volume Encryption Management".

E	n	c	r	y	p	t		V	o	l	u	m	e	?	
→	Y	e	s			N	o								

When the configuration is finished, the server name and IP address will be shown. If the NAS fails to create the disk volume, the following message will be shown.

C	r	e	a	t	i	n	g	.	.	.					
R	A	I	D	5		F	a	i	l	e	d				

## **View system information by the LCD panel**

When the LCD panel shows the server name and IP address, you may press the "Enter" button to enter the Main Menu. The Main Menu consists of the following items:

1. TCP/IP
2. Physical disk
3. Volume
4. System
5. Shut down
6. Reboot
7. Password
8. Back

### **1. TCP/ IP**

In TCP/ IP, you can view the following options:

- 1.1 LAN1 IP Address
- 1.2 LAN1 Subnet Mask
- 1.3 LAN1 Gateway
- 1.4 LAN 1 PRI. DNS
- 1.5 LAN 1 SEC. DNS
- 1.6 Enter Network Settings
  - 1.6.1 Network Settings – DHCP
  - 1.6.2 Network Settings – Static IP\*
  - 1.6.3 Network Settings – BACK
- 1.7 Back to Main Menu

\* In Network Settings – Static IP, you can configure the IP address, subnet mask, gateway, and DNS of LAN 1 and LAN 2.

## 2. Physical disk

In Physical disk, you can view the following options:

- 2.1 Disk1 Info
- 2.2 Disk2 Info
- 2.3 Disk3 Info
- 2.4 Disk4 Info
- 2.5 Disk5 Info
- 2.6 Disk6 Info
- 2.7 Back to Main Menu

The disk info shows the temperature and the capacity of the hard drive.

D	i	s	k	:	1		T	e	m	p	:	5	0	°	C
S	i	z	e	:		2	3	2		G	B				

## 3. Volume

This section shows the disk configuration of the NAS. The first line shows the RAID configuration and storage capacity; the second line shows the member drive number of the configuration.

R	A	I	D	5						7	5	0	G	B
D	r	i	v	e		1	2	3	4					

If there is more than one volume, press the "Select" button to view the information. The following table shows the description of the LCD messages for RAID 5 configuration.

LCD Display	Drive configuration
RAID5+S	RAID5+spare
RAID5 (D)	RAID 5 degraded mode
RAID 5 (B)	RAID 5 rebuilding
RAID 5 (S)	RAID 5 re-synchronizing
RAID 5 (U)	RAID 5 is unmounted
RAID 5 (X)	RAID 5 non-activated

#### 4. System

This section shows the system temperature and the rotation speed of the system fan.

C	P	U		T	e	m	p	:		5	0	°	C		
S	y	s		T	e	m	p	:		5	5	°	C		

S	y	s		F	a	n	:	8	6	5	R	P	M		

#### 5. Shut down

Use this option to turn off the NAS. Press the "Select" button to select "Yes". Then press the "Enter" button to confirm.

#### 6. Reboot

Use this option to restart the NAS. Press the "Select" button to select "Yes". Then press the "Enter" button to confirm.

#### 7. Password

The default password of the LCD panel is blank. Enter this option to change the password of the LCD panel. Select "Yes" to continue.

C	h	a	n	g	e		P	a	s	s	w	o	r	d	
					Y	e	s		<input type="checkbox"/>	N	o				

You may enter a password of maximum 8 numeric characters (0-9). When the cursor moves to "OK", press the "Enter" button. Verify the password to confirm the changes.

N	e	w		P	a	s	s	w	o	r	d	:			
														O	K

#### 8. Back

Select this option to return to the main menu.



## System Messages

When the NAS encounters system error, an error message will be shown on the LCD panel. Press the "Enter" button to view the message. Press the "Enter" button again to view the next message.

S	y	s	t	e	m	E	r	r	o	r	!			
P	l	s	.		C	h	e	c	k		L	o	g	s

System Message	Description
Sys. Fan Failed	The system fan failed
Sys. Overheat	The system overheat
HDD Overheat	The hard drive overheat
CPU Overheat	The CPU overheat
Network Lost	Both LAN 1 and LAN 2 are disconnected in Failover or Load-balancing mode
LAN1 Lost	LAN 1 is disconnected
LAN2 Lost	LAN 2 is disconnected
HDD Failure	The hard drive fails
Vol1 Full	The volume is full
HDD Ejected	The hard drive is ejected
Vol1 Degraded	The volume is in degraded mode
Vol1 Unmounted	The volume is unmounted
Vol1 Nonactivate	The volume is not activated

## Technical Support

QNAP provides dedicated online support and customer service via instant messenger. You can contact us by the following means:

Online Support: <a href="http://www.qnap.com/online-support.asp">http://www.qnap.com/online-support.asp</a> E-mail: <a href="mailto:q_support@qnap.com">q_support@qnap.com</a> MSN: q.support@hotmail.com SKYPE: qnapskype
---

### Technical support for North America users:

E-mail: <a href="mailto:support@usa.ieiworld.com">support@usa.ieiworld.com</a> 1-800 Hotline: 866-276-6754 ext.110 Address: 168 UNIVERSITY PARKWAY POMONA, CA 91768-4300
--

# GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>  
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## Preamble

---

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the

source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

## **TERMS AND CONDITIONS**

---

### **0. Definitions.**

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

## **1. Source Code.**

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

## **2. Basic Permissions.**

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

### **3. Protecting Users' Legal Rights From Anti-Circumvention Law.**

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's

users, your or third parties' legal rights to forbid circumvention of technological measures.

## **4. Conveying Verbatim Copies.**

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

## **5. Conveying Modified Source Versions.**

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive



interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

## **6. Conveying Non-Source Forms.**

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified

object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

## **7. Additional Terms.**

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

## **8. Termination.**

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

## **9. Acceptance Not Required for Having Copies.**

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

## **10. Automatic Licensing of Downstream**

### **Recipients.**

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

## **11. Patents.**

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

## **12. No Surrender of Others' Freedom.**

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.



## **13. Use with the GNU Affero General Public License.**

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

## **14. Revised Versions of this License.**

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

## **15. Disclaimer of Warranty.**

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

## **16. Limitation of Liability.**

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## **17. Interpretation of Sections 15 and 16.**

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS